WORLD ECONOMIC FORUM

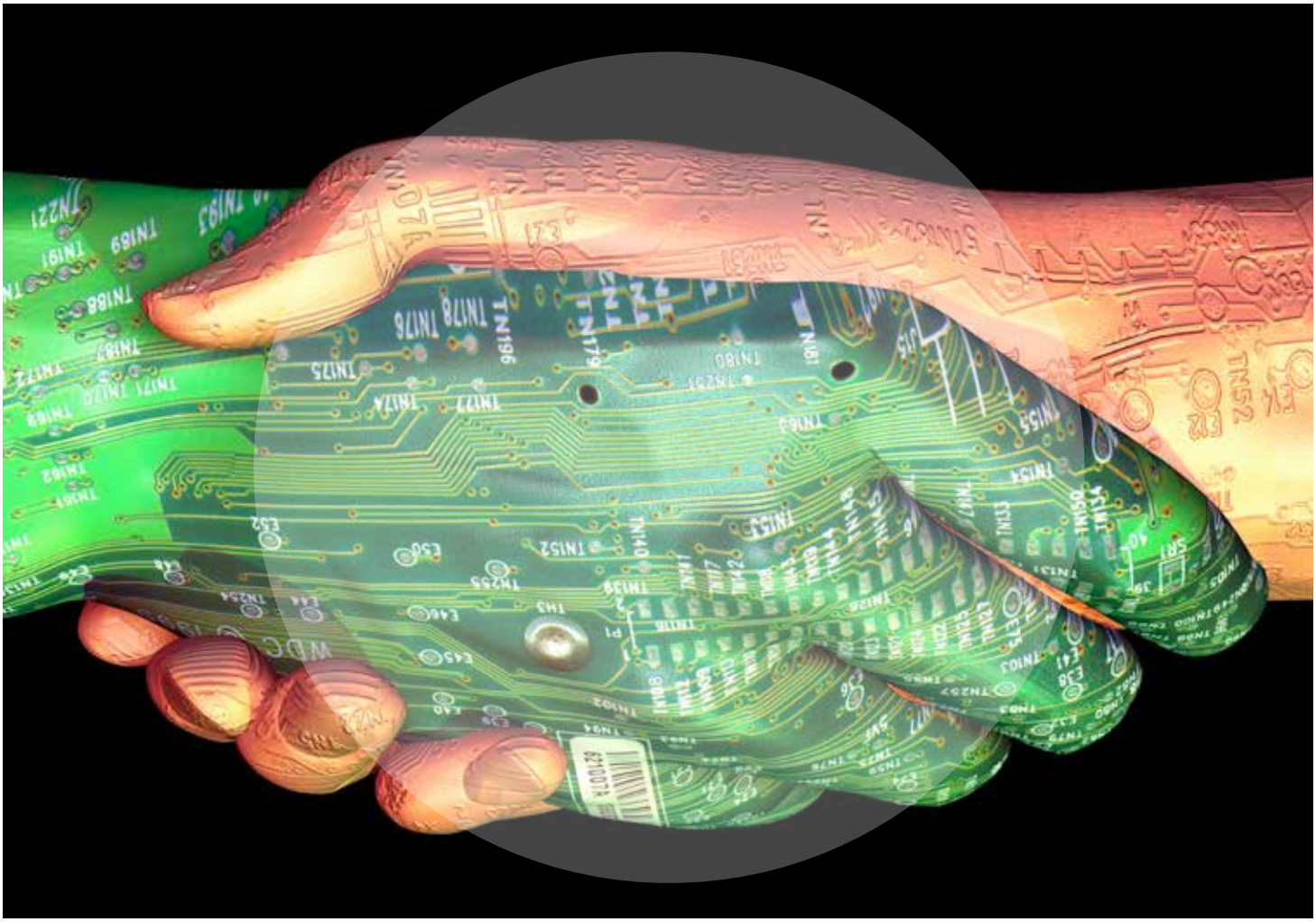
COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

Risk and Responsibility in a Hyperconnected World

In collaboration with McKinsey & Company

January 2014



Contents

2 Executive Summary

5 Introduction

Chapter 1. Developing a Clear Set of Action Areas

7 Institutional Readiness

9 Public and International Policy

10 Community Responses

10 Systemic Responses

Chapter 2. Findings: Understanding Cyber Risks and Response Readiness

11 For most companies across sectors and regions, cyber resilience is a strategic risk

15 Executives believe they are losing ground to attackers

15 Large companies lack the facts and processes to make effective decisions about cyber resilience

18 Concerns about cyberattacks are starting to have measurable negative business implications in some areas

18 Substantial actions are required from all players in the cyber resilience ecosystem

Chapter 3. Future Scenarios

27 Scenario One: Muddling into the Future

27 Scenario Two: Backlash Decelerates Digitization

27 Scenario Three: Cyber Resilience Accelerates Digitization

27 Applying the Scenarios

Chapter 4. Conclusions and Roadmap for Collaborative Action

Executive Summary

Many leaders in business, civil society and government realize that for the world's economy to fully derive the value inherent in technological innovation, a robust, coordinated system of global cyber resilience is essential to effectively mitigate the risk of cyberattacks. This view is beginning to permeate discussions among senior leaders in the private and public sectors, and across different industries, as concerns related to cyber resilience shift from awareness to action. The critical questions today are: what needs to be done, and how can it be achieved?

Risk and Responsibility in a Hyperconnected World, a joint effort between the World Economic Forum and McKinsey & Company, assesses the necessary action areas, and examines the impact of cyberattacks and response readiness. The report sets these against three alternative scenarios in which economic value from technological innovations is realized or lost depending on models of cyber resilience. It draws on knowledge and opinions derived from a series of interviews, workshops and dialogues with global executives and thought leaders to estimate the potential value to be created through 2020 by technological innovations. It examines the value that could be put at risk if the adoption of such innovations is delayed because more frequent, intense cyberattacks are not met with more robust cyber resilience. Finally, the report draws conclusions from the analysis and research, and offers a 14-point roadmap for collaboration.

Chapter 1. Developing a Clear Set of Action Areas presents a unified agenda for key action areas that global leaders across the spectrum of private and public sectors and civil society can collectively explore to increase cyber resilience. Based on the interviews, workshops and dialogues with senior global executives and thought leaders, this chapter is intended to serve as an ongoing, evolving resource to be continually developed and improved over time.

Discussions to date have produced a series of action areas for leaders to consider, organized as required solutions.

Chapter 2. Findings: Understanding Cyber Risks and Response Readiness examines at key findings from the interviews and workshops, with a particular focus on institutional readiness.

Pervasive digitization, open and interconnected technology environments, and sophisticated attackers, among other drivers, mean that the risk from major cyber events could materially slow the pace of technological innovation over the coming decade. Addressing the problem will require collaboration across all participants in the "cyber resilience ecosystem". But many questions remain on direction and responsibilities. In contrast, a much clearer picture is emerging of the actions that institutions should take to protect themselves. They should act now to enhance capabilities while a broader model for resiliency develops. Finally, given the strategic decisions required, chief executive officers (CEOs), government ministers and other key stakeholders from civil society must engage directly with one another to put the right policies and plans in place.

Findings from the research include:

- Risks of cyberattacks are starting to have a business impact. Controls put in place to protect information assets have at least a "moderate" impact on front-line employee productivity for nearly 90% of institutions. Moreover, security concerns are already making companies delay implementation of cloud and mobile technology capabilities. And while direct cyber resilience spend represents only a small share of total enterprise technology expenditure, some chief information officers (CIOs) and chief information security officers

(CISOs) estimate that indirect or unaccounted security requirements drive as much as 20-30% of overall technology spending, crowding other projects that could create business value.

- Current trends could result in a backlash against digitization, with huge economic impact. Major technology trends like massive analytics, cloud computing and big data could create between US$ 9.6 trillion and US$ 21.6 trillion in value for the global economy. If attacker sophistication outpaces defender capabilities – resulting in more destructive attacks –a wave of new regulations and corporate policies could slow innovation, with an aggregate economic impact of around US$ 3 trillion.

- Large institutions lack the facts and processes to make and implement effective decisions about cyber resilience. Overall, a large majority of firms have only nascent or developing cyber risk management capabilities. Most large institutions do not systematically understand which information assets need to be protected, who are their attackers, what is their risk appetite or which is the most effective set of defence mechanisms. Companies that spend more on cyber resilience do not necessarily manage cyber resilience risks in a more mature way – many are simply throwing money at the problem.

- More collaboration required, but key questions remain. Almost all CIOs and CISOs say they cannot "do it alone". They believe a broader cyber resilience ecosystem must be put in place that spans not only the enterprise users of technology, but also technology providers, regulators, law enforcement and other related institutions. However, views vary widely on the responsibilities and effectiveness of several possible public-sector actions.

Chapter 3. Future Scenarios presents three alternative settings for 2020, and is based on the opinions and thoughts gleaned from the interviews and extensive workshop sessions. The scenarios estimate the conceivable value created from technological innovations that could be affected by a changing cyber resilience environment:

- *Scenario One:* Muddling into the Future. In this baseline scenario, attackers retain an advantage over defenders who continue to respond to threats reactively, albeit successfully. The level of threat increases incrementally, and more sophisticated attack tools consistently leave defenders behind attackers. Adoption of innovative technologies slows. In this scenario, as much as US$ 1.02 trillion in value from technological innovation is left unrealized over the next five to seven years.

- *Scenario Two:* Backlash Decelerates Digitization. In this scenario, the frequency of attacks significantly escalates, and international cooperation to combat the proliferation of attack tools proves elusive. Government cyber resilience regulations become more directive, disturbing adoption of innovative technologies. As much as US$ 3 trillion in potential value creation from these technologies remains unrealized.

- *Scenario Three:* Cyber Resilience Accelerates Digitization. In this scenario, proactive action from the public and private sectors limits the proliferation of attack tools, builds institutional capabilities and stimulates innovation. A vital cyber resilience ecosystem serves to facilitate and connect company operations. Technological innovation is enabled, accelerating digitization and creating between US$ 9.6 trillion and US$ 21.6 trillion in value over the remainder of this decade.

Chapter 4: Conclusions and Roadmap for Collaborative Action proposes a framework for collaboration and suggests a path forward. Acknowledging the interdependence of the public and private sectors in today's hyperconnected milieu, the Forum's Partnership for Cyber Resilience, launched in 2012, has developed a framework to help chief executives and other leaders to build effective cyber risk management platforms. The tool offers a rough composite score to locate an organization on the five stages of maturity. By assessing their positions on the maturity scale, companies can make the necessary plans and take the necessary action to enhance their cyber resilience. A core Forum team and its partners will enable and advise participants in their approach to cyber risk management. The team also will be a storehouse for insights garnered from participants that can be used to build up the framework for broader sharing.

TABLE 1: FOUR CATEGORIES

1 Institutional readiness	**Governance** Prioritize information assets based on business risks and integrate cyber resilience into enterprise-wide risk management
	Program development Differentiate protection based on importance of assets. Develop deep integration of security into technology environment. Deploy active defenses to uncover attacks proactively. Continuous testing to improve incident response and enlist front-line personnel
	Network development Coordinate better with partners, vendors, and other counterparts to effectively mitigate network risk
2 Public and international policy	**National cyber strategy** Establish a comprehensive, transparent national cyber strategy that integrates procedures across all policy domains
	End-to-end criminal justice system Ensure that law enforcement and the state have a comprehensive and flexible legal code and capabilities to take action
	Domestic policy and incentives Establish private, public, and civil dialogue to develop suitable policy and market mechanisms
	Foreign policy Establish a national cyber strategy. Identify institutions and critical capabilities and harmonize policies through multi-stakeholder collaboration
	Public goods Encourage multi-stakeholder collaboration to invest in capabilities, capacity and resources for the public good
3 Community	**Research** Invest in research to better understand the cyber landscape and threats
	Information sharing Work to promote better information sharing by further developing collaboration tools and resources
	Shared resources for capability building Foster partnerships between governments, universities, and the private sector to develop capabilities and capacity
4 Systemic	**Risk markets** Explore and invest to develop risk markets and value risks from cyber events
	Embedded security Work to better integrate security into current technology systems and tools

Introduction

Digital technology touches virtually every aspect of daily life today. Social interaction, healthcare activity, political engagement or economic decision-making – digital connectivity permeates it all, and the dependence on this connectivity is growing swiftly. Greater reliance on a networked resource naturally makes us more interdependent on one another. As the new, shared digital space evolves, the collective imperative is to develop a common set of expectations to address systemic risks, and to define not only the roles but also the responsibilities of all participants in the cyber ecosystem. The obligations will encompass several key issues – from privacy norms to Internet governance policy – but the collective ability to manage cyber risks in this shared digital environment is fundamental. It forms the crux of cyber resilience.

But as the nature of cyber threats is evolving, so should the approach to cyber resilience. Three observations help to put this in context:

1. Cyber resilience is not an isolated issue. Cyber resilience is part of a much broader transformation across society driven by information and communication technologies. The term "digital hyperconnectivity" refers to the increasing or exponential rate at which people, processes and things are connecting to the Internet. This results in some key shifts:

- The impact of technology shifts from improving efficiency to enabling transformation of business operations and institutions.
- The structure of systems changes fundamentally, away from hierarchies towards networks.
- Disintermediation offers huge social and economic gains, but presents new governance and assurance challenges.

2. Cyber resilience is not a single issue. When referring to cyber resilience or cybersecurity, it is easy to assume that a single topic or issue is meant. However, these terms refer to a set of issues that are as varied as they are distinct. One Internet may connect people, but the challenges are several. In the "real" world, retail fraud, organized crime, invasions of personal privacy, diplomacy, warfare, intellectual property and copyright violations, terrorism and activism happen in very different ways, and different governance mechanisms (such as institutions, treaties, regulations and market mechanisms) have evolved to deal with each of them. Of course, part of the challenge of the "virtual" world is that these mechanisms in their current form are not reliable. Designed in a pre-digital world, they move too slowly and ignore the digital age's interdependencies. Indeed, in many cases, even the underlying values and concepts cannot be depended upon – the digital era has re-constituted ideas such as privacy, ownership and security. The common notion of security implies isolation, the protection of a defined perimeter or an objective defined by the prevention of an event. This notion of security seems quaint in a world where it is impossible to draw a clean ring around the network of one country or one company, and where large organizations can be the target of 10,000 cyberattacks per day.

3. Cyber resilience is a socio-economic issue. Most critically, the realization is growing that cyber resilience is also a socio-economic issue, although it has been more commonly recognized as a technical and political issue.

From the digitally enabled car to smart cities, from energy infrastructure to air travel, from cashless banking to on-the-spot market prices for farmers in developing economies, humankind is witnessing an explosion of innovation in technology. This groundswell of creativity is not centred solely in Silicon Valley, but is occurring across industries everywhere. The phenomenon has massive potential to generate economic value. And many of its gains in recent years have derived directly from digital global connectivity.

Discussions of cyber risks tend to focus on doomsday scenarios or a feared "cybergeddon". However, an equivalent concern perhaps should be the lost opportunities from a significant backlash or fragmentation of the current digital ecosystem. A backlash could result from a single major event, or through gradual erosion. Governments, businesses or individuals could cause it. Fragmentation could occur intentionally, as loss of trust leads to explicitly isolationist policies. Or it could occur semi-intentionally, as governments adopt increasingly protectionist stances on digitally enabled services. Or it could occur unintentionally, as uncoordinated policy developments in different jurisdictions result in a disparate set of requirements to operate globally.

Risk and Responsibility in a Hyperconnected World examines the link between responses to cyber resilience concerns and the creation of real economic value. If cyber resilience is a potential risk to growth and competitiveness, it is also an enabler. Countries and companies that invest in and develop cyber capabilities to instil trust in customers, citizens and investors will have a c ompetitive edge in this digital era. This report also outlines the key action areas for leaders across private, public and civil society to drive collective cyber capabilities and resilience.

FROM A BROAD DATA SET WE BUILT FUTURE SCENARIOS, ESTIMATED IMPACT AND DEVELOPED POTENTIAL ACTIONS

Fact base

Interviews with industry leaders

- Conducted 250+ interviews with industry leaders across
  - 7+ sectors (e.g., FS[1], healthcare)
  - 3 regions (Americas, EMEA[2], and Asia), and
  - 5+ roles (e.g., CISOs, CIOs, CTOs, CROs, VPs)
- Captured responses of industry leaders (subset of above) to questionnaire assessing risks and implications of cybersecurity

Cyber risk maturity survey (CRMS)

- Compared cyber resilience of 100+ large firms (primarily >$5B market cap) with best-practices across
  - Multiple sectors (primarily FS and healthcare)
  - 3 regions (Americans, EMEA, Asia), and

Experience from client engagements

- Developed business-focused cyber resilience strategies, operating models, vendor strategies and conducted realistic cyber-event simulations to improve responses to real attacks with the world's largest firms and institutions

Cyber resilience drivers

- Leveraged fact base from interviews, CRMS, and experience to develop, prioritize, and synthesize list of 20+ drivers that impact cyber resilience

Alternative future scenarios

- Derived 3 alternative future scenarios based on realistic varied outcomes of synthesized cyber resilience drivers

Deliverables for Davos 2014

Estimated global economic impact

- Estimated impact of cyber resilience to adoption of significant business and technology innovations in 3 alternative future scenarios
  - List of key business and technology innovations and their value
  - Impact to adoption of business and technology innovations estimated through interviews with industry leaders

Potential actions

- Developed a set of coordinated actions for private- and public-sector stakeholders to improve cyber resilience across four areas
  - Institutional readiness
  - Information sharing
  - Critical infrastructure
  - Policy development

[1]Financial Services
[2]Europe, Middle East and Asia

Chapter 1. Developing a Clear Set of Action Areas

As the risk of cyberattacks is becoming more prevalent, the cost of the attacks – to companies, public institutions, the global economy and society at large – is also growing. This is the clear message that emerged from research assembled over the past year. To foster technology innovation, and continue to reap value from it, a robust cyber resilience ecosystem is required across sectors and institutions. To deter malevolent attackers, companies will have to abandon their current fragmented cyber resilience defences built around reactive "audit" and "compliance" models. Today's increasingly digital age needs a step-change in cyberattack response – cyber resilience models that are characterized by a business-driven, risk-management approach.

The Partnership for Cyber Resilience, launched at the World Economic Forum Annual Meeting 2012 in Davos-Klosters, identified three vital areas of robust cyber resilience: information-sharing, critical infrastructure protection, and policy development. During the past year, the group's dialogue set a context for these vital areas within a broader readiness framework aimed at building collaboration and coordination. Institutional readiness and the potential action to improve it, form the first of four pillars of this broader structure. The others include public and international policy, community action and systemic action.

The latest work, which included interviews, workshops and surveys, has shown that a range of high-value responses exists upon which to build a vigorous cyber resilience capability at the institutional level. This group of institutional readiness responses comprises governance issues, program development and network expansions for private-sector institutions. On the one hand, these responses address an immediate need of executives for specific steps to shore up their companies' current cyber resilience capabilities and establish critical benchmarks. On the other, the responses can form the core of a cyber resilience model that, over time, can foster companies' collaboration with partners in public and international policy, as well as community and systemic responses. Strengthening the core is an essential first step to developing effective responses on a broader scale.

1. Institutional Readiness

Governance

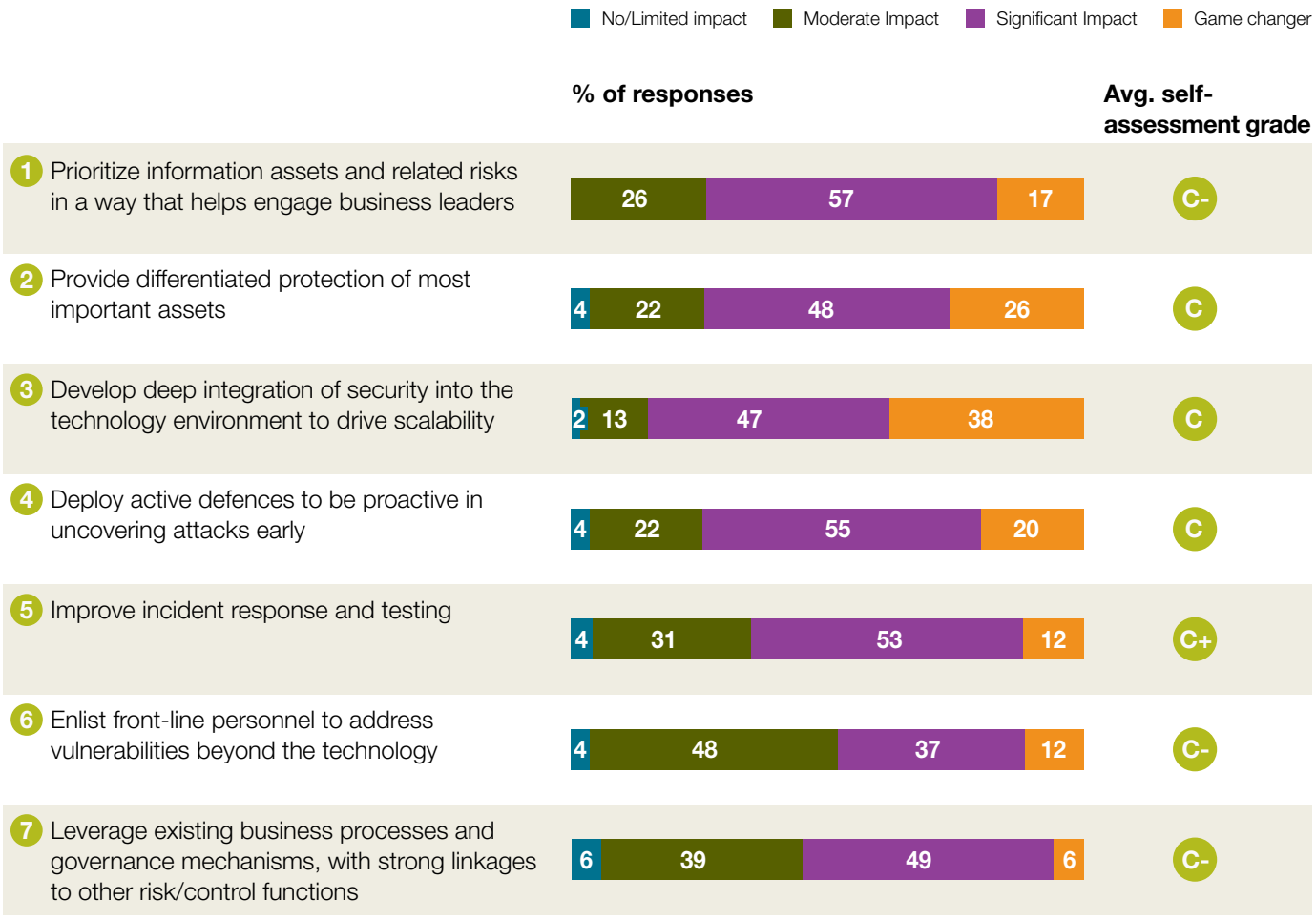
- **Prioritize information assets based on business risks.** Most institutions lack sufficient insight into the precise information assets they need protected and how to assign priorities to those assets. Going forward, cyber resilience teams need to work with business leaders to better understand business risks (for example, what it means to lose proprietary information about a new manufacturing process) across the entire value chain and to set appropriate priorities to the underlying information assets.
- **Develop deep integration of security into the technology environment to drive scalability.** Almost every part of the broader technology environment has an impact on an institution's ability to protect itself, from application development practices to policies for replacing out-dated hardware. Institutions must move from "bolting security on" to training their entire staff to incorporate security from the start into technology projects.

Program/network development

- **Provide differentiated protection based on the importance of assets.** As the axiom states, "To protect everything is to protect nothing." By implementing differentiated controls, such as encryption and more rigorous passwords, institutions can focus time and resources on protecting information assets that matter the most.
- **Deploy active defences to uncover attacks proactively.** Massive amounts of information are available about potential attacks – both from external intelligence sources and from an institution's own technology environment. Increasingly, companies will need to develop capabilities to aggregate and analyse relevant information, and use it to appropriately tune defence systems such as firewalls.
- **Test continuously to improve incident response.** An inadequate response to a breach – not only from the technology team, but also from those in marketing, public affairs or customer services – can be as damaging as the breach itself because of the adverse reaction it can elicit from clients, partners, government regulators and others. Taking a page from the military, institutions should run cross-functional "cyberwar games" to improve their ability to respond effectively in real time.
- **Help personnel to understand the value of information assets.** Users are often the biggest vulnerability for an institution. They click on links they should not, select insecure passwords and send sensitive files by e-mail to broad distribution lists. Institutions need to segment users, and help each group to understand the business risks of the information assets they touch every day.

FIGURE 1: POTENTIAL ACTIONS TO IMPROVE INSTITUTIONAL READINESS

What actions that your institution could take would have the most impact in reducing the risk associated with cyberattacks?
(%)



Source: Interviews of chief information security officers and other executives, World Economic Forum and McKinsey & Company

- **Integrate cyber resistance into enterprise-wide risk management and governance processes.** Cyber resilience is an enterprise risk, and must be managed like one. Assessments of risks from cyberattack must be i ntegrated with other risk analysis and presented at relevant management and board discussions. Cyber resilience implications must be integrated into the broad set of enterprise governance functions such as human resources, vendor management and regulatory compliance.

The importance of these actions was highlighted in interviews with chief information security officers (CISOs) and other executives. Across the board, executives gave their institutions poor average marks for executing these critical responses (see Figure 1). As a group, these institutional readiness actions can also serve as benchmarks and form a core of expanded cyber resilience collaboration with the public sector and communities.

2. Public and International Policy

The public sector has a responsibility to act to address the growing cyber threat. As such, cyber resilience should be made part of relevant policies or systems such as a national cyber strategy, an end-to-end criminal justice system, domestic and foreign policy, and laws for the public good.

National strategy. Lack of national coordination can lead to redundant policy and legislation, thereby hindering economic growth and development. The Research produced certain recommendations:

- Each nation connected to the Internet should have a comprehensive and transparent national cyber strategy that is integrated and harmonized with the strategies and procedures across all domestic and international policy.
- As each body and organization has a role, it is crucial that the strategies developed incorporate the private and civil sectors, as well as leverage economic and security issues, among other tools, to drive the adoption of initiatives. The focus on incentives driven by the government and independent providers should be enhanced.
- Finally, a competent institution is needed to be responsible for the successful implementation and rollout of the national strategy. An identifiable, responsible institution will offer transparency to stakeholders in the process. Not having a resource to consult often leads to challenges of ownership, function and action, the research highlighted.

End-to-end criminal justice system. "Institutions can take all the actions they want on their own. However, if there is no law-enforcement mechanism to pursue and prosecute perpetrators, then our actions are meaningless," a chief information officer (CIO) observes in an interview. Indeed, law enforcement needs to have the capability and resources to investigate cybercrimes and to have an appropriate, comprehensive and agile legal code to support its investigative and prosecutorial activities. Cyber resilience is a complex matter that may not be entirely clear to everybody in the criminal justice system. As such, it is critical that legal advocates, either through further education or other training, understand the cyber resilience ecosystem well enough to carry out due process.

> **Institutions can take all the actions they want on their own. However, if there is no law-enforcement mechanism to pursue and prosecute perpetrators, then our actions are meaningless.**
>
> Chief information officer of a financial services organisation

Domestic policy. No clear consensus emerged in the Forum-McKinsey workshops and dialogues on the nature of public-sector action needed domestically. Based on the background and regulatory history of the participants, it seemed that different sectors had different views on the most beneficial action. As such, two key points are identified:

- **Private, public and civil dialogue is needed to develop a coherent mix of policy and market mechanisms for use in the cyber ecosystem.** Not taking a multistakeholder approach risks eliciting a mix of responses that could be weighted unevenly in one area, resulting in limited success.
- **A rapidly changing cyber resilience landscape requires all government mechanisms to support the efforts of law enforcement and to be appropriately agile.** It was emphasized during a December 2013 roundtable discussion of partners in Washington DC that a major impediment to potential public-sector actions would be a rigid set of codes that did not allow changes to a highly dynamic sector.

Foreign policy. "Cyberattacks have the potential to change the nature of warfare and international relations, almost past the level of the Cold War," says the CIO of a European aerospace and defence company. It is clear that cyber events are changing the nature of interstate relations. As such, countries should establish a **national cyber doctrine** to define and express their positions on the use of cyber resilience tools and weapons for national purposes.

The workshops and dialogues showed that today different organizations are sharing information and cooperating on cyber actions. **Communication, formal and informal, is essential among those investigating, prosecuting and enforcing laws on cybercrime.** Making the process transparent can help to cut the confusion and lag in tracking and prosecution. In addition, each level of government is responsible for identifying competent authorities and for creating interoperability among national entities and sovereign legal codes. For businesses to continue to expand, **better harmonization of national policies** will be needed.

All these requirements reiterate the need for a multistakeholder approach to address cyber risks. A primary concern voiced by several institutions is the often-stark differences in requirements for different nations. This challenge can drastically affect the growth of international and local businesses.

Public good. For the public good, all stakeholders need to ensure that they contribute to and maintain an evolving and robust incident-response capability. This ranges from established programs for information-sharing and incident response such as CERT (Computer Emergency Readiness Team) to information training and development of human resources. Such a dynamic space demands an ever-evolving set of capabilities to match the changing pace of the threat. Maintenance includes possible funding for cyber resilience research and greater investment in cyber resilience technical education in order to foster a more cyber-aware workforce.

3. Community Responses

In cyber resilience components where public and private interests intersect, it is vital for the community to agree and act as one. This is particularly important for infrastructure, which often accommodates many interests. The community can cooperate on actions such as: research, information-sharing, knowledge transfer, self-governance, sharing resources for capability building, and mutual aid.

Research. Cyber resilience or cybersecurity is still a fairly nascent topic, and requires further investment from interested parties to be fully understood and developed. As such, it is important to encourage public- and private-sector efforts to better understand the impact of cyber resilience on enterprises, nations and macroeconomics. This common language development would be helpful in setting priorities and focusing government policies on cyber resilience. Many advancements in this space occurred outside formal institutions. As such, it will be important to create an atmosphere in which counter-attack ("white-hat hacker") research is not only encouraged but also supported financially.

Shared resource for capability building. Foster partnerships among governments, universities and the private sector to develop skills in this area.

Information-sharing. As one of the core areas of focus identified by the Partnership for Cyber Resilience in 2012, key recommendations surfaced regarding sharing of information:

- Where legally feasible, institutions need to find mechanisms for information-sharing already in existence, either formally or informally.
- Towards that end, it will be critical to improve the quality of the ISACs/CERTs/CIERTs and other information-sharing venues to provide the best variety of options.
- The success of such programs requires the promotion of an interoperable, extensible and automated system for sharing information.

4. Systemic Responses

A series of actions can greatly improve the quality of conversation on cyber resilience and accelerate coordination. Although thinking on this issue continues to evolve, two areas offer promise in building maturity in the ecosystem:

- **Risk markets**. Making use of a developed cyber risk insurance market to trade and monetize the risk from cyber events.
- **Embedded security.** Exploring options to embed security parameters earlier into the lifecycle of products, and even into contemporary means of communication, such as the Internet.

Against this backdrop of high-value responses, it is worth noting that another range of actions is likely to deliver low or uncertain value in fostering cyber resilience. For example, while governments may be in a position to disrupt supply chains for attack vectors, such a move by private-sector institutions would seem to be uncertain or counter-productive because of the collateral fallout. For their part, regulators may be able to engage in counter-attacks and service disruptions, but they should be cautious about allowing Internet service providers to engage in similar efforts because of possible reprisals on the overall infrastructure or bystander organizations.

Chapter 2. Findings: Understanding Cyber Risks and Response Readiness

Cyber resilience is becoming a critical business and social issue. As more and more business value and personal information rapidly migrates to digital form, the risks from cyberattacks grow ever more daunting. On the front line are public and private institutions that rely on cyber resilience systems and controls to protect intellectual property, information assets and business continuity. Supporting them are regulators who develop the policies to facilitate and defend technology, law enforcement agencies, and industry associations that work to share information and improve institutional security.

Defying all of them are cyberattackers, with a wide range of motives and sophisticated tools to access or disrupt cyber services. Criminals pursue financial gain through online fraud or theft of identity. State-sponsored actors engage in online espionage and sabotage. Competitors steal intellectual property or interrupt business to grab advantage. Online "hactivists" pierce firewalls to disturb functions or make political statements. Often, insiders help the external attackers or initiate their own attacks, worsening the odds for institutions.

Eliminating threats from sophisticated malevolent players is impossible. Other factors also complicate the response. Open and interconnected technology environments make historic "protect the perimeter" strategies insufficient and, in many cases, counter-productive. As mentioned earlier, much of the damage is caused by inadequate response to the breach, rather than the breach itself. Moreover, mitigating the impact of attacks and ruptures often implies complicated trade-offs between risk reduction and business impact. Large institutions struggle with cyber resilience decisions because quantifying risks and its alleviation is difficult, and getting executive engagement on trade-offs is practically impossible.

Cyber resilience is the successful mitigation of the strategic and economic impacts of cyberattacks, and is based on cybersecurity capabilities. This chapter assesses the options for participants in the security ecosystem to increase cyber resilience. These findings are gleaned from the workshops held over 2013 and the interviews with more than 200 industry leaders in seven sectors across the Americas, Europe, the Middle East and Africa, and Asia.[2] The workshops and interviews focused on three topics: practitioner views on the importance of cyber risks; the impact of attacks on businesses, the effect of cyber risks on investment in research and development (R&D) and efforts to mitigate risk; and potential mitigating actions. The interviews were augmented with survey data that compared cyber resilience capability in large firms with best practices across multiple sectors and regions. Some critical findings from the research include:

1. For most companies across sectors and regions, cyber resilience is a strategic risk

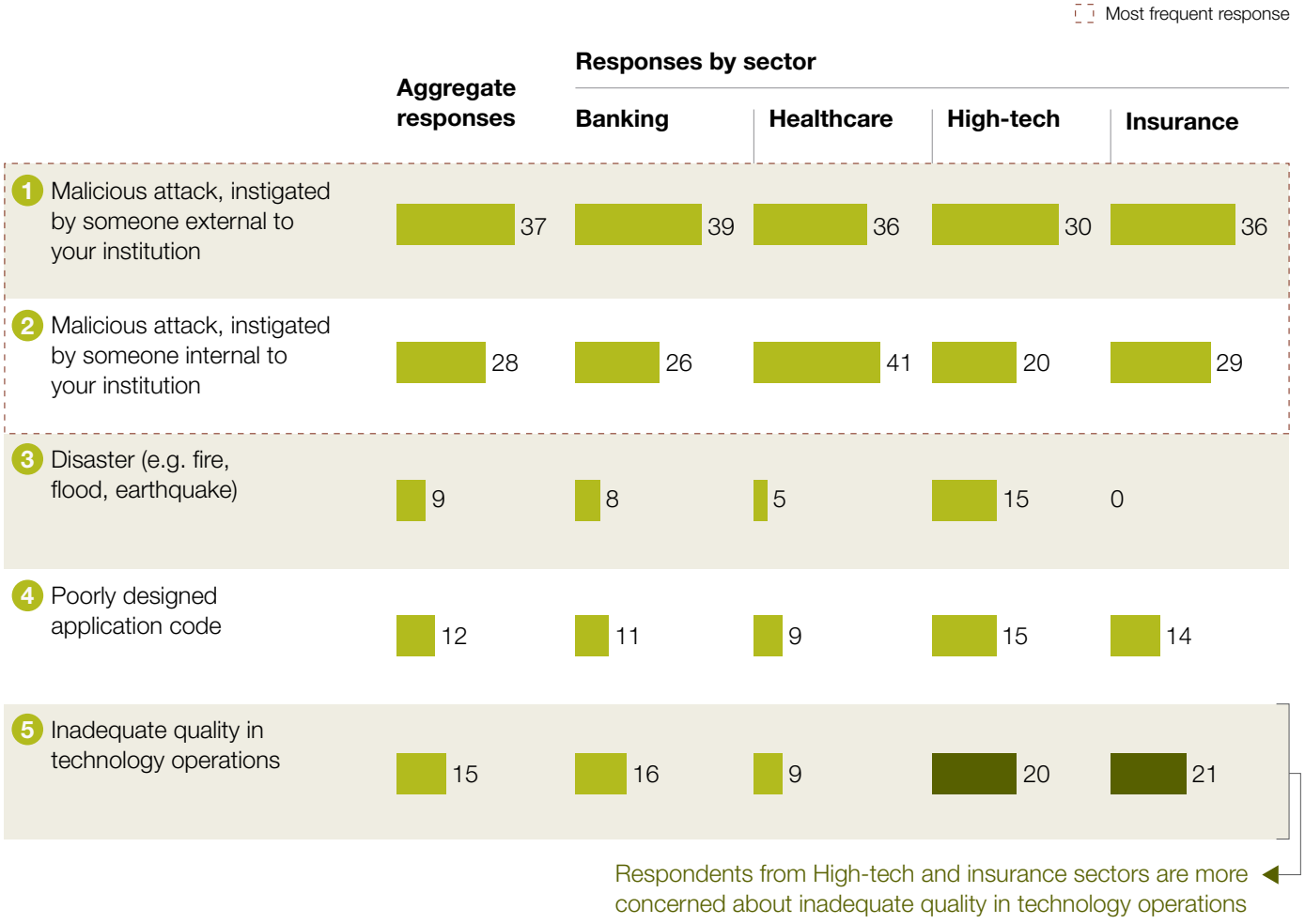
The workshop and interview sessions found that European companies are slightly more concerned than their American counterparts about cyber resilience. The research also indicated that as awareness has grown, chief information officers (CIOs) and chief technology officers (CTOs) are just as concerned as chief Information security officer (CISOs). Practitioners believe cyberattacks are a greater risk than other types of technology risks. Some executives found internal threats to be as big a risk as external attacks (see Figure 2).

Financial institutions are particularly sensitive — about 80% of them believe cyber resilience is a "strategic risk", compared with roughly half of other institutions. "The issue is coming earlier in the conversation," says the chief executive officer (CEO) of a high-tech vendor. "Before, we may not have covered it until the end of the meeting; now it is the first or second thing companies are asking us about." (See Figure 3.)

The nature of the threat is heavily dependent on sector. "Product" companies, such as those in high technology, are most concerned about industrial espionage. "Services" companies focus on the loss and release of personally identifiable information and service disruption. Concern also exists over interference with business operations over time. For product companies, the leaking of proprietary knowledge about production processes may be more damaging than leaks of product specifications, given the pervasiveness of "tear down" techniques and legal protection for product designs.

FIGURE 2: CYBERATTACKS ARE MORE OF A RISK

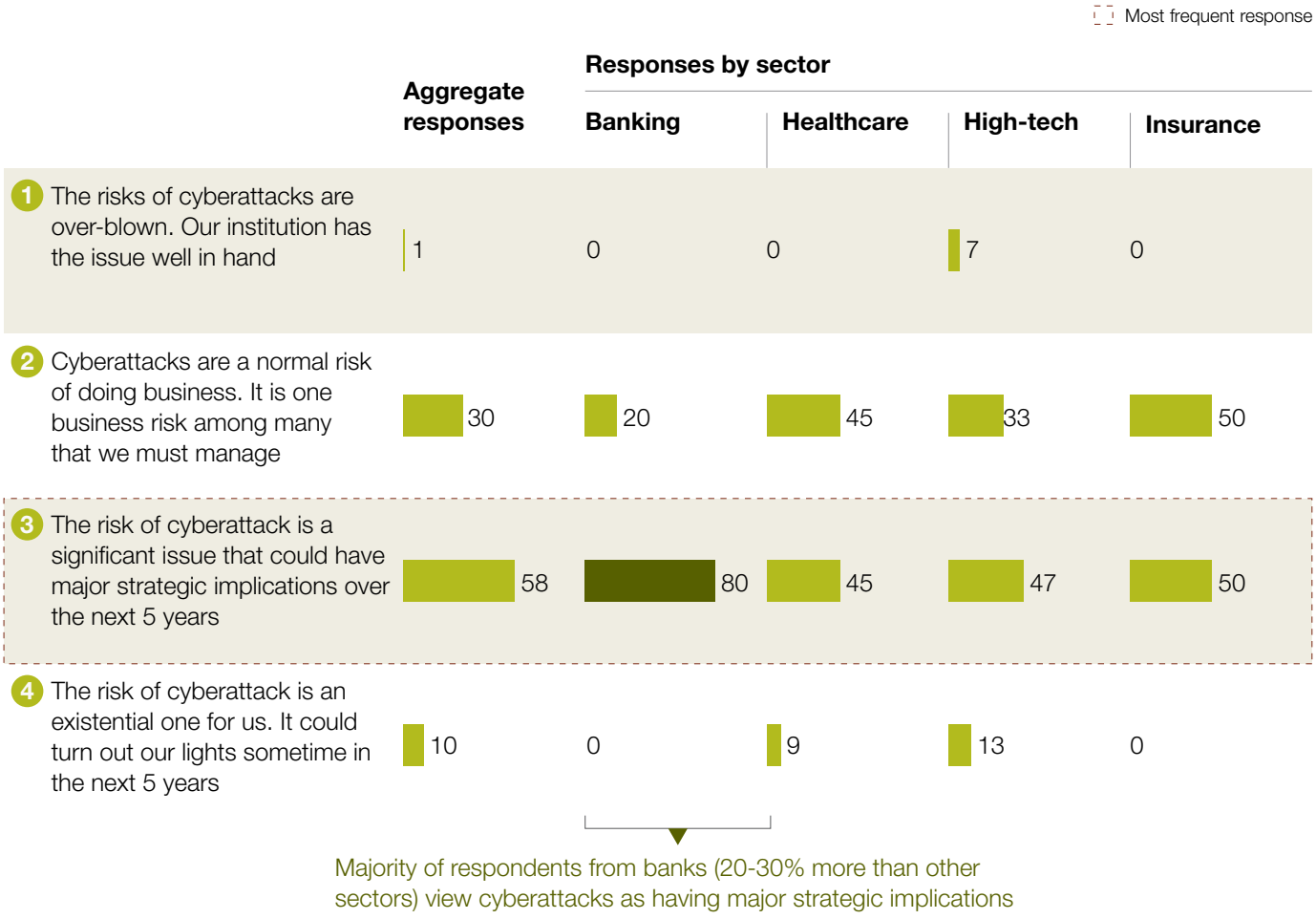
Interview question: What type of technology risks are most likely to have a strategic and negative impact on your business?
% of respondents who rated response 1-2 on scale of 5



Source: Industry leader interviews; team analysis, World Economic Forum and McKinsey & Company

FIGURE 3: OVERWHELMING MAJORITY OF FINANCIAL INSTITUTIONS CONSIDER CYBERSECURITY TO BE A STRATEGY RISK

Interview question: How would you describe your level of concern about intentional internal or external threats to the confidentiality, integrity & availability of your company's data and information systems?
% of respondents



Source: Industry leader interviews; team analysis, World Economic Forum and McKinsey & Company

Thinking about Risks

On June 11-12, 2013, over 100 participants gathered at the World Economic Forum's headquarters in Geneva to discuss strategic risks.

As part of the programme, the Partnership for Cyber Resilience hosted two breakout sessions on:

- Macroeconomic trends in the cyber ecosystem
- Potential solution sets for individual institutions and systemically

As sample set of macroeconomic drivers and trends were established as part of the scenario develop process and included:

- Motivations, such as level of distrust, interstate tensions, corporate IP theft and deterrents to cyber crime
- Mechanisms, including the democratization of technology and the balance between offensive and defensive technology
- Mitigations, such as the sophistications of institutions, interstate cooperation and sophistication of users

The group also began to explore potential solution sets aligned against the three priority areas that were recommended during the previous year:

- Information sharing
- Critical infrastructure
- Policy development

The community used this opportunity to begin to consider components of a potential next generation cyber operating model.

Jeff Moss, Vice-President and Chief Security Officer, ICANN

Guha Ramasubramanian, Head, Business Development, Wipro

Rod Beckstrom, Chief Security Advisor, Samsung

Michael Fertik, CEO and Founder, Reputation.com

2. Executives believe they are losing ground to attackers

Equally worrisome, a large majority of participants in the interviews and workshops believe that attackers will continue to increase their lead over defenders. About 69% of interviewees say that the sophistication or pace of attackers will increase quicker than the ability of institutions to defend. "[The attackers] need to get lucky once and have the ability to evolve so rapidly," says an executive in the pharmaceuticals sector. "Our large company just isn't agile enough to match [their] pace." Of particular concern is the dissemination of sophisticated hacking and attack programs. To date, state entities have managed to control attack programs aimed at disrupting their victims' operations and activities. But executives worry that such programs will make their way to a wider variety of attackers with more destructive intent. Says the CISO of a hospital network: "It is the ultra silent spyware and sophisticated attackers that have been the real threat to us. We just don't have the resources to counter what is next." (See Figure 4.)

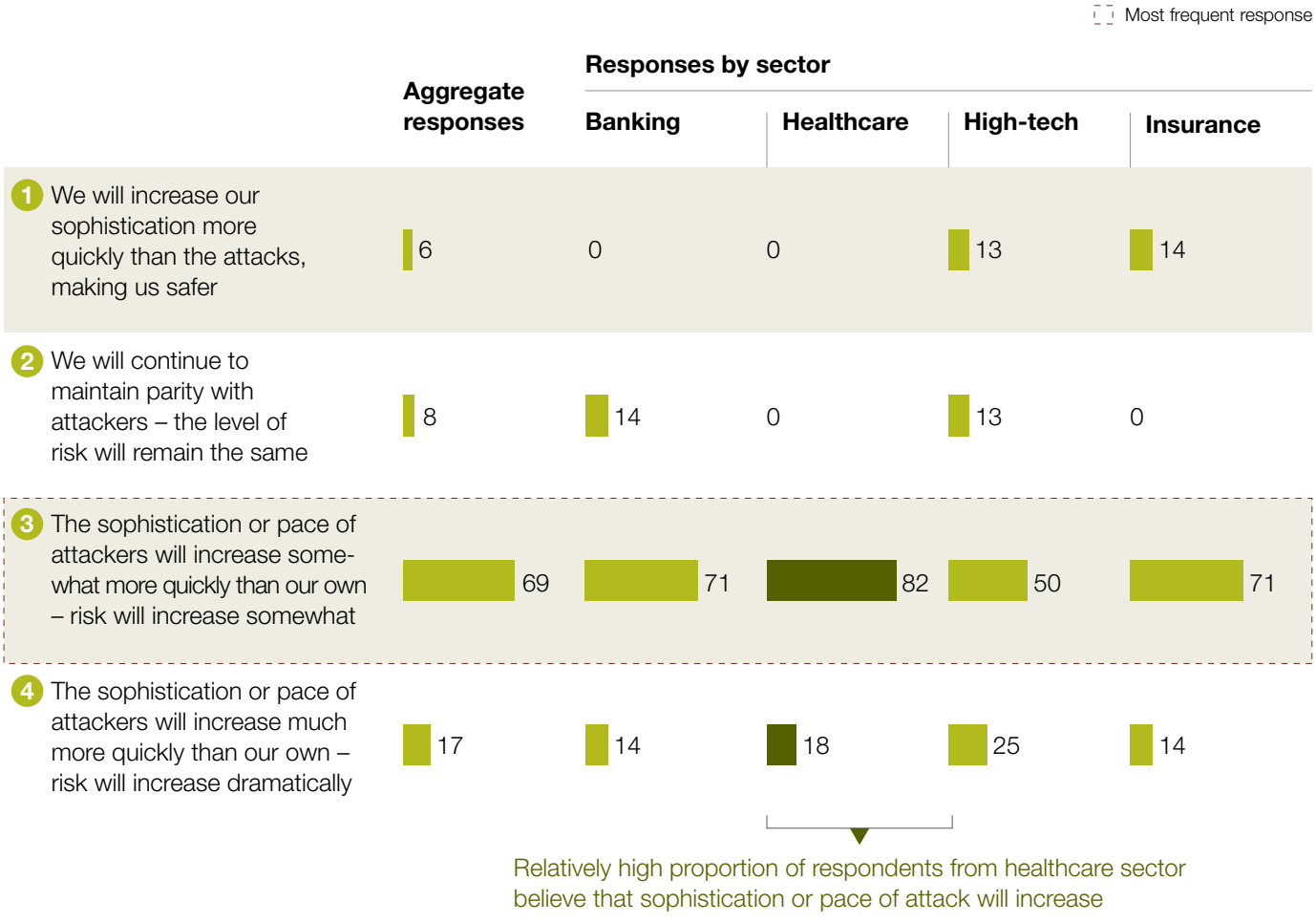
3. Large companies lack the facts and processes to make effective decisions about cyber resilience

A survey conducted in parallel to augment the interviews points to gaps across sectors in current risk management capabilities. Of the 100 companies whose cyber risk management processes were examined, 90% had "nascent" or "developing" risk management capabilities. Only 21% were rated "mature" or better on four or more of the eight practice areas studied. (See Figure 5.)

Institutions can be segmented based on the sophistication of their risk management capabilities and the scale of their cyber resilience expenditure. Spending and enterprise maturity are not correlated, however. "Unprotected" companies spend little and spend it poorly. Others punch above their weight by spending little but doing a better job of risk management. Still others, the "well-protected", spend vigorously and have relatively good capabilities for extracting value from their investment. Finally, some seem to throw resources at the problem, spending a great deal without much risk management sophistication. (See Figure 6.)

Figure 4: Majority of executives believe attackers will increase lead over defenders.

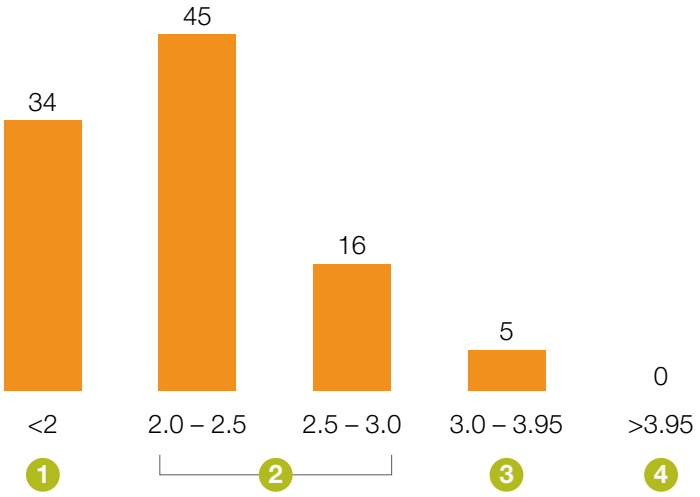
Interview question: How do you believe the relative level of sophistication will evolve for your institution compared to potential attackers over the course of the next 5 years?
% of respondents



Source: Industry leader interviews; team analysis, World Economic Forum and McKinsey & Company

FIGURE 5: MAJORITY OF FIRMS HAVE NASCENT OR DEVELOPING CYBER RISK MANAGEMENT CAPABILITIES

Distribution of overall cyber risk management maturity scores [1-4]
% of firms



- Only 21% of respondents were rated "mature" or better on 4 or more of the 8 practice areas
  - Only 5% rated "mature" or better overall
  - No organizations at top overall rating of "robust"
- Only one respondent was "mature" or better in every practice area
- 34% of respondents were "nascent" or "developing" in at least 4 of 8 areas

1 Nascent
- Best effort based evaluation and mitigation of cyber risks
- No defined single point of accountability nor a clearly defined escalation path to top management

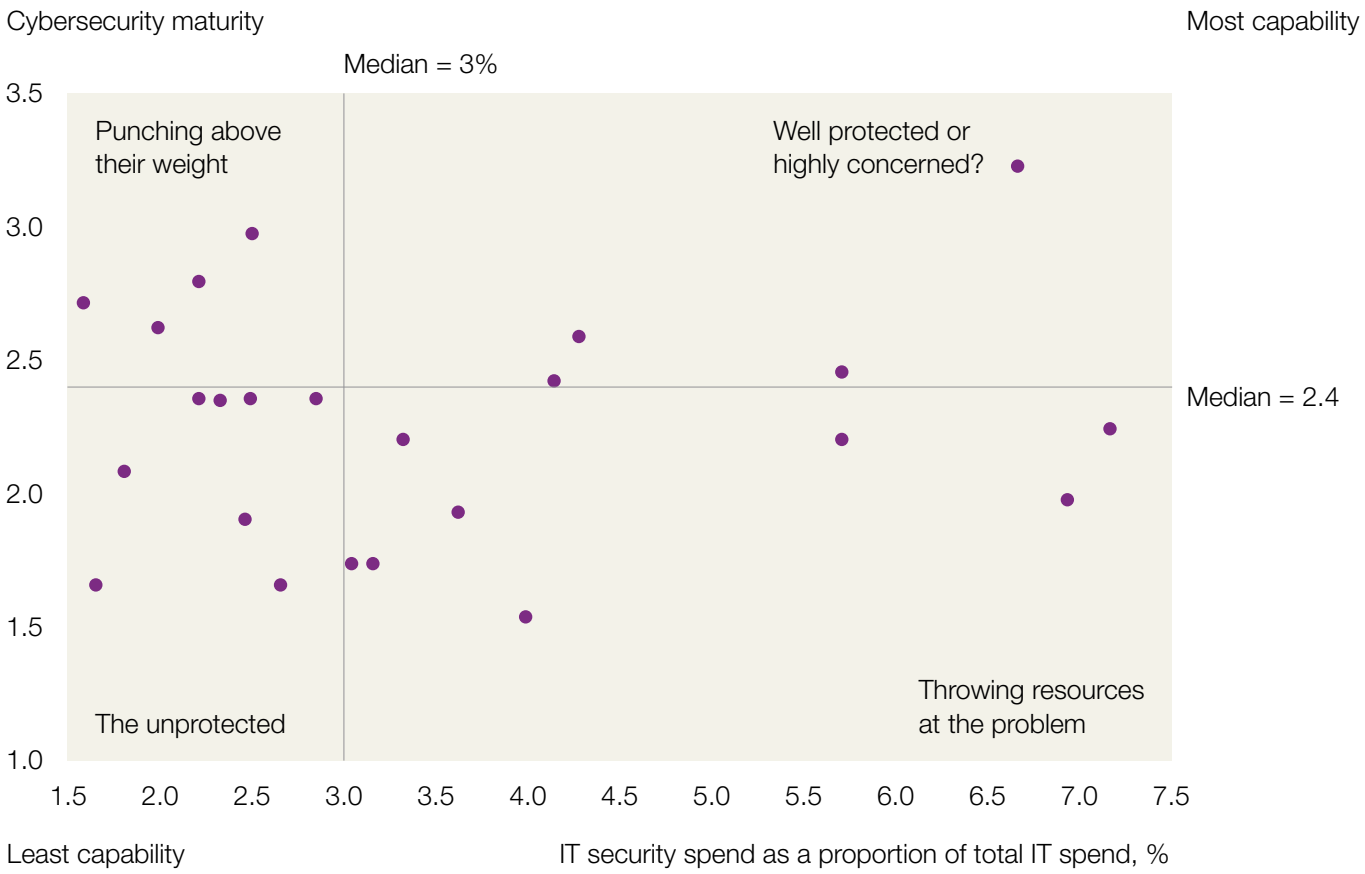
2 Developing
- Mostly qualitative framework for evaluating and mitigating cyber risks
- Overall consistent governance model and known single point of accountability in each BU with a defined reporting line to top management

3 Mature
- Quantitative approach for evaluating and qualitative approach for mitigating cyber risks
- Defined cybersecurity governance model with a single point of accountability within a BU that owns the risks and decision-making

4 Robust
- Robust quantitative approach for evaluating and mitigating cyber risks
- Clearly identified individuals accountable for cybersecurity of each asset

Source: McKinsey Cyber Risk Maturity Survey (CRMS)

FIGURE 6: CYBERSECURITY MATURITY



Source: McKinsey Cyber Risk Maturity Survey (CRMS)

The workshops and other research found that banking is slightly more mature than other sectors in cyber resilience capabilities. The largest companies across sectors also are slightly more mature than smaller ones. Variations within a sector and a size band are much larger than variations between sectors and between size bands. Even the largest firms have substantial room for improvement. For example, while financial services organizations tend to be more mature than other sectors, senior non-technical executives still struggle to incorporate cyber risk management into enterprise risk management discussions, and often are unable to make informed decisions because of lack of data.

4. Concerns about cyberattacks are starting to have measurable negative business implications in some areas

Speed, mobility and collaboration are the hallmarks of the successful company in the digital age. But as cyberattacks proliferate, executives have to devote more attention to protecting vulnerable operations, often by imposing controls that create friction in critical functions. So far, cyberattacks appear to have had only a limited impact on R&D plans, except at high-tech firms. Only about 25% of surveyed executives in banking and healthcare, and 17% in insurance, say that they would have to change the nature of their R&D investments to retain their value in the face of cyberattacks even if their underlying intellectual property is stolen. In the high-tech sector, fully half say they would have to change the nature of their R&D efforts over time.

Concern is apparent, however, about cyberattacks slowing value capture from cloud computing, mobile technologies and some healthcare technologies. About 78% of companies surveyed say security concerns delayed adoption of public cloud computing by a year or more, and 43% note that such concerns delayed enterprise mobility capabilities by a year or more. “We have started to experiment with mobile devices,” says the chief security officer (CSO) of a financial institution. “However, the delay has been mainly because there are too many potential threats.” In healthcare, concerns about cyber resilience are not delaying the adoption of most technologies, though large hospital networks report that security issues have led to postponing the introduction of connected medical devices by up to a year. “Most devices have no security applications on them at all,” says another hospital’s CISO. “Anyone can just get in and manipulate whatever they want.”

Cyber resilience controls are having a significant impact on front-line productivity. About half of companies overall said that controls had at least a moderate impact on end-use productivity. Half of the high-tech executives cited existing controls as “a major pain point” for users and as limiting the ability of employees to collaborate. (See Figure 7.)
Actual spending on cyber resilience may also be much higher than most executives assume, the research indicates. “Indirect” spending on information technology (IT) security to adjust to new risks and provide ongoing responses to cyber risks may be a significant cost driver for IT organizations. Direct IT security spending ranged from 2% to 10% of total IT spend in the companies researched. But chief Internet strategy officers estimated incremental activity driven by security requirements at between 2% and 25% of total IT spend.
In general, insurance and healthcare executives believe they spend too little on cybersecurity. Banking and high-tech executives say their spending on cybersecurity is about right. (See Figure 8.)

5. Substantial actions are required from all players in the cyber resilience ecosystem

It is broadly agreed that to reduce the overall level of threat from cyberattacks the biggest impact would come from a combination of efforts involving policy-makers, industry associations such as the Financial Services Information-sharing Analysis Center and individual institutions. (See Figure 9.)

Solution building with public and private institutions

On December 12th, 2013, the initiative hosted 30 representatives of the public and private sector to discuss and finalize a set of areas of action at the US Department of Homeland Security. As part of the discussion, the group discussed four main buckets:

- Institutional actions
- International and public policy
- Community
- Systemic

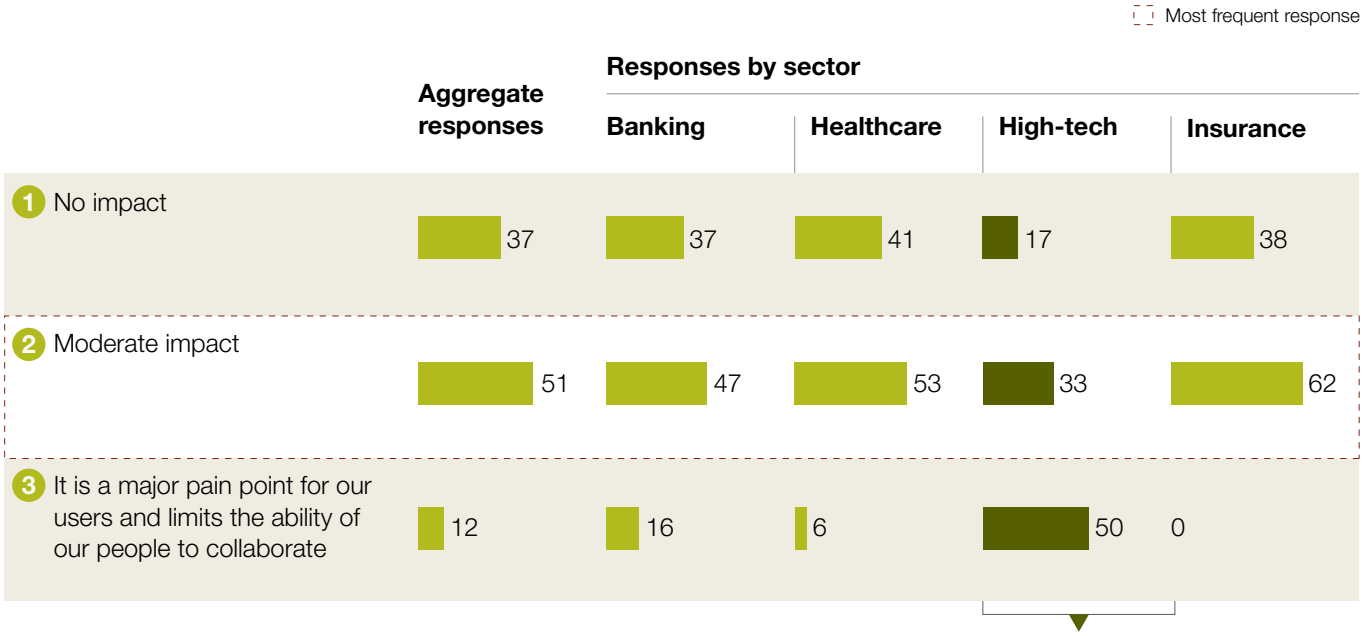
Participants outlined specific recommendations within each of the categories including:

- The need for all institutions to improve their institutional capabilities through an agreed upon set of next generation operating model principles,
- A need for public sector organizations to work to harmonize action and policy both within their institutions but also globally,
- The importance of a common global language when discussing cyber risks and for collective actions for the public good,
- and, the need to explore potential systemic changes to the way risks are mitigated and accounted for in the global marketplace.

These amongst other conversations served as the basis for the framework for collaborative actions.

FIGURE 7: IMPACT OF CYBERSECURITY CONTROLS ON FRONT-LINE PRODUCTIVITY

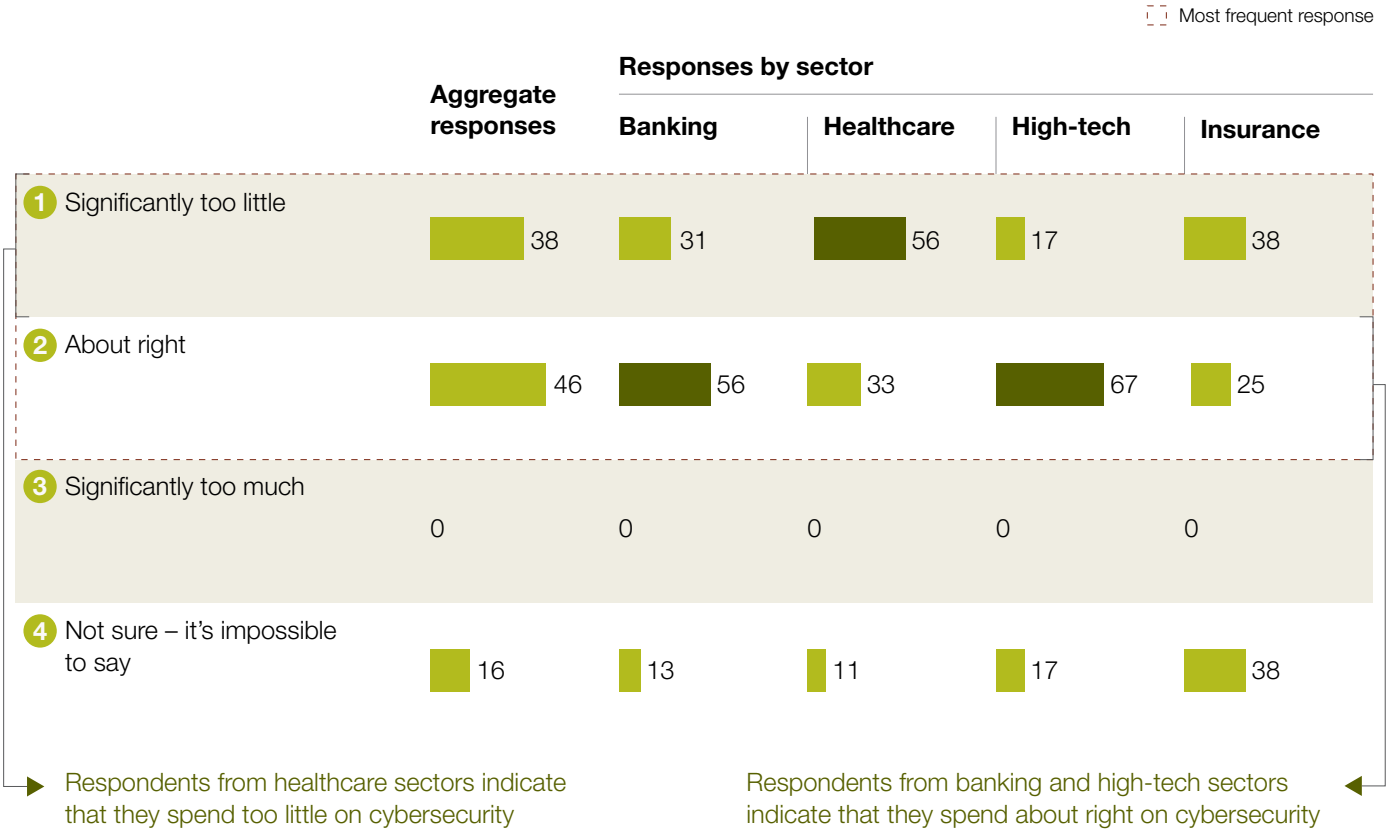
Interview question: How much impact do controls related to cybersecurity (e.g. document encryption, limitations placed on use of mobile devices) have on front-line productivity?
% of respondents



Source: Industry leader interviews; team analysis, World Economic Forum and McKinsey & Company

FIGURE 8: SPENDING ON CYBERSECURITY

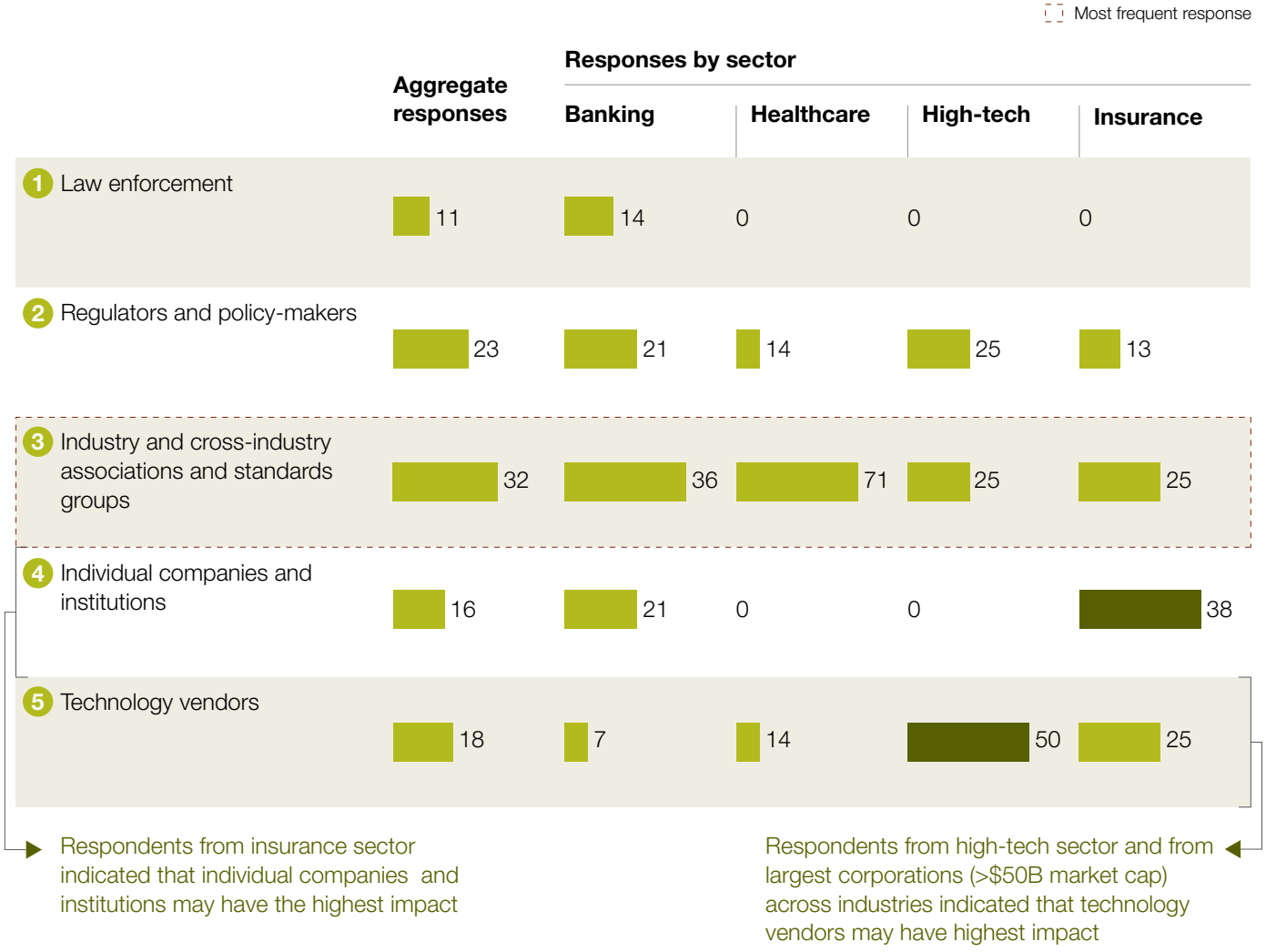
Interview question: What is your perspective on how much your company spends on cybersecurity, given current level of maturity?
% of respondents



Source: Industry leader interviews; team analysis, World Economic Forum and McKinsey & Company

FIGURE 9: COMBINATION OF EFFORTS WOULD BE MOST USEFUL

Interview question: Who could have the most impact in reducing overall level of threat associated with cyberattacks in your sector?
% of respondents



Source: Industry leader interviews; team analysis, World Economic Forum and McKinsey & Company

But considerable disagreement exists about how such a consensus could take shape. Relationships between private and public institutions are unformed in many cases. Consensus is limited across industries, and across the private and public sectors. Insurance executives indicate that individual companies and institutions may have the strongest impact in fending off cyber risks. Respondents from the high-tech sector and from the largest corporations – those with a market cap of more than US$50 billion – indicate that technology vendors may be in a position to have the strongest impact.

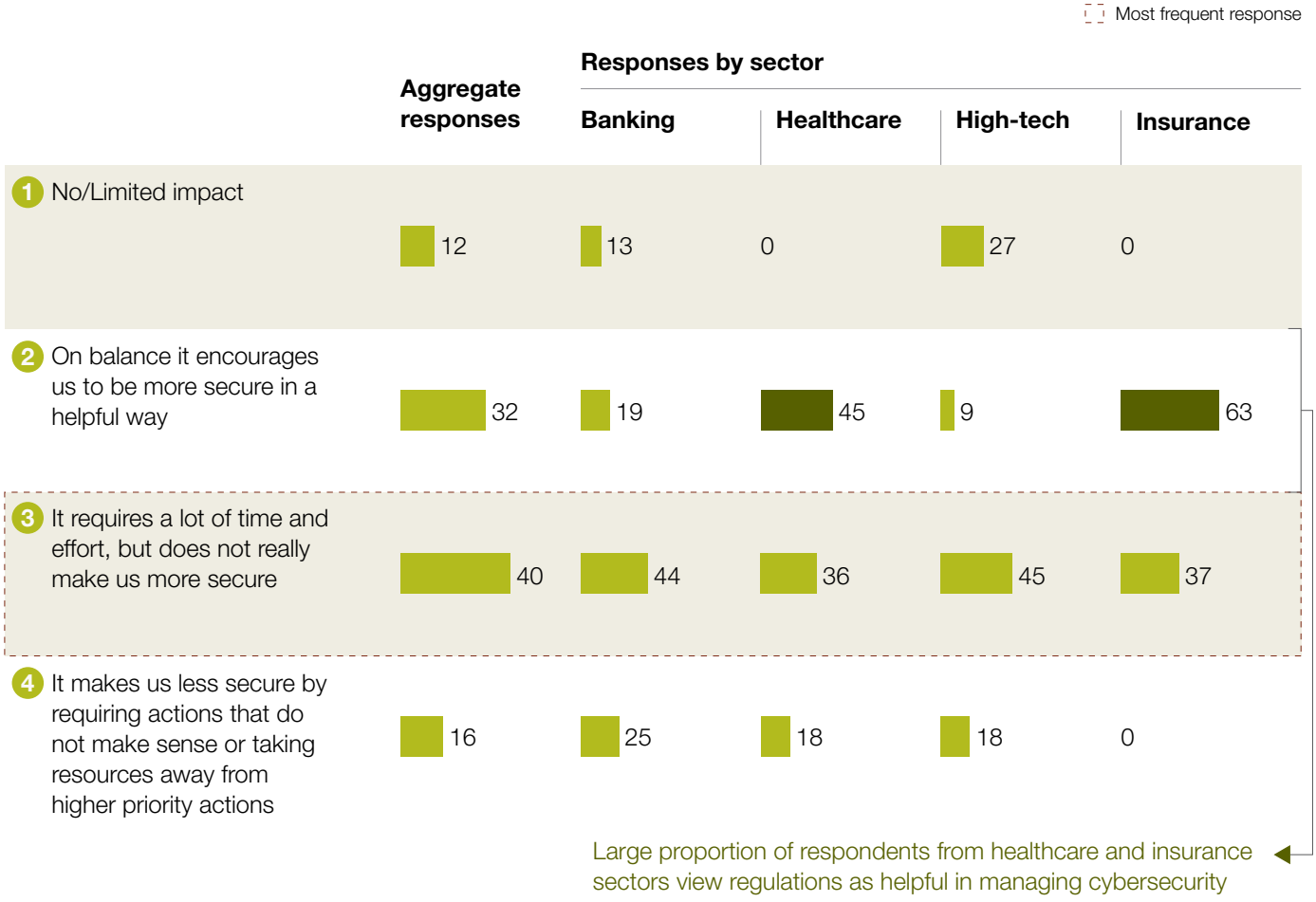
Similarly, the perception of regulation varies widely, depending on sector. Consensus is lacking on which public-sector actions would be most beneficial. Executives worry that broad agreement regulations can lock in outdated techniques, and that regulators lack the skills and capabilities to provide effective input. Financial-services technology executives say that regulation is actively harmful because it forces a focus on the wrong things. Yet a large proportion of respondents from the healthcare and insurance sectors view regulations as helpful in managing cyber resilience. Healthcare technology executives say regulation is not ideal but remains valuable because it compels senior management to commit attention and resources to security issues. "Institutionally, we can take all the actions we want but the threat will only be reduced when governments and law enforcement agencies are able to take action," says the CISO of a pharmaceutical company. (See Figure 10.)

Traditional approaches also appear increasingly ineffective. In most cases businesses rely mainly on passive measures, typically addressing issues only after they have arisen. Business partners are not sufficiently involved, and policing and application of cyber resilience lack consistent rigour. Responses are often backward looking, require specialized talent that is costly and hard to find, and rely mostly on technology solutions, even though sophisticated agents often attack the weakest link: customers and employees.

Still, the research finds near universal agreement among CSOs, CTOs and CISOs that a step-change improvement is needed in their own capabilities to protect their businesses from increasingly sophisticated cyber threats, enable productivity and innovation, and maintain a competitive cost position. Says the CISO of a global bank: "You have some at the top and some that are clueless, but the bulk are in the middle and they are behind" (i.e. below the median). Adds the cyber resilience chief of a national law enforcement agency: "Some businesses have really improved their position, but more need to take [cyber resilience] as a business issue overall and really need to improve their resilience."

FIGURE 10: IMPACT OF CYBER RESILIENCE

Interview question: What impact does government regulation have on your ability to manage cybersecurity related risks?
% of respondents



Source: Industry leader interviews; team analysis, World Economic Forum and McKinsey & Company

SCENARIOS TESTING AT THE ANNUAL MEETING OF THE NEW CHAMPIONS

During the World Economic Forum Annual Meeting of New Champions 2013 in Dalian, People's Republic of China, senior business leaders and executives convened at a private session to explore current and future potential drivers and trends that will define the cyber ecosystem. They also took a look at how each of the drivers would come together to form four potential scenarios by 2020:

- Scenario A: Cyber threats increase, but sophistication of institutions does not. Businesses continue to reach the way they have in the past and the attack vendors continue to group together and increase in their relative sophistication.

- Scenario B: Fears about cyber security slow down cooperation and trust. Sophisticated attack vectors are disseminated to a wider range of actors with some harboring truly destructive intent. This ripples into implications for consumer purchasing habits, limiting business strategies and severely inhibiting government regulations

- Scenario C: Technology and security become enablers to growth. Governments come together in the face of an ever increasing threat to facilitate the dramatic uplift in institutional capability and international cooperation.

- Scenario D: After destructive attacks, public-private cooperation is improved, but consumer trust is eroded. A series of highly visible, destructive attacks shake the bedrock of consumer purchasing habits, forcing businesses to shift the way the act.

Participants discussed the implications of each of the scenarios. Some of the themes that emerged included:

- A push for new and innovative solutions from third party vendors to help combat newer and more sophisticated threats
- A need to reformulate business strategy to consider changes ranging from countries in which companies feel comfortable operating in to the way they connected with consumers
- A need for greater regional and international cooperation
- between nations to align regulations as well as prosecute criminals
- Opportunities will emerge for new businesses in insurance or risk markets to help businesses mitigate the potential downside from cyber risks

Participants of the Partnership for Cyber Resilience session

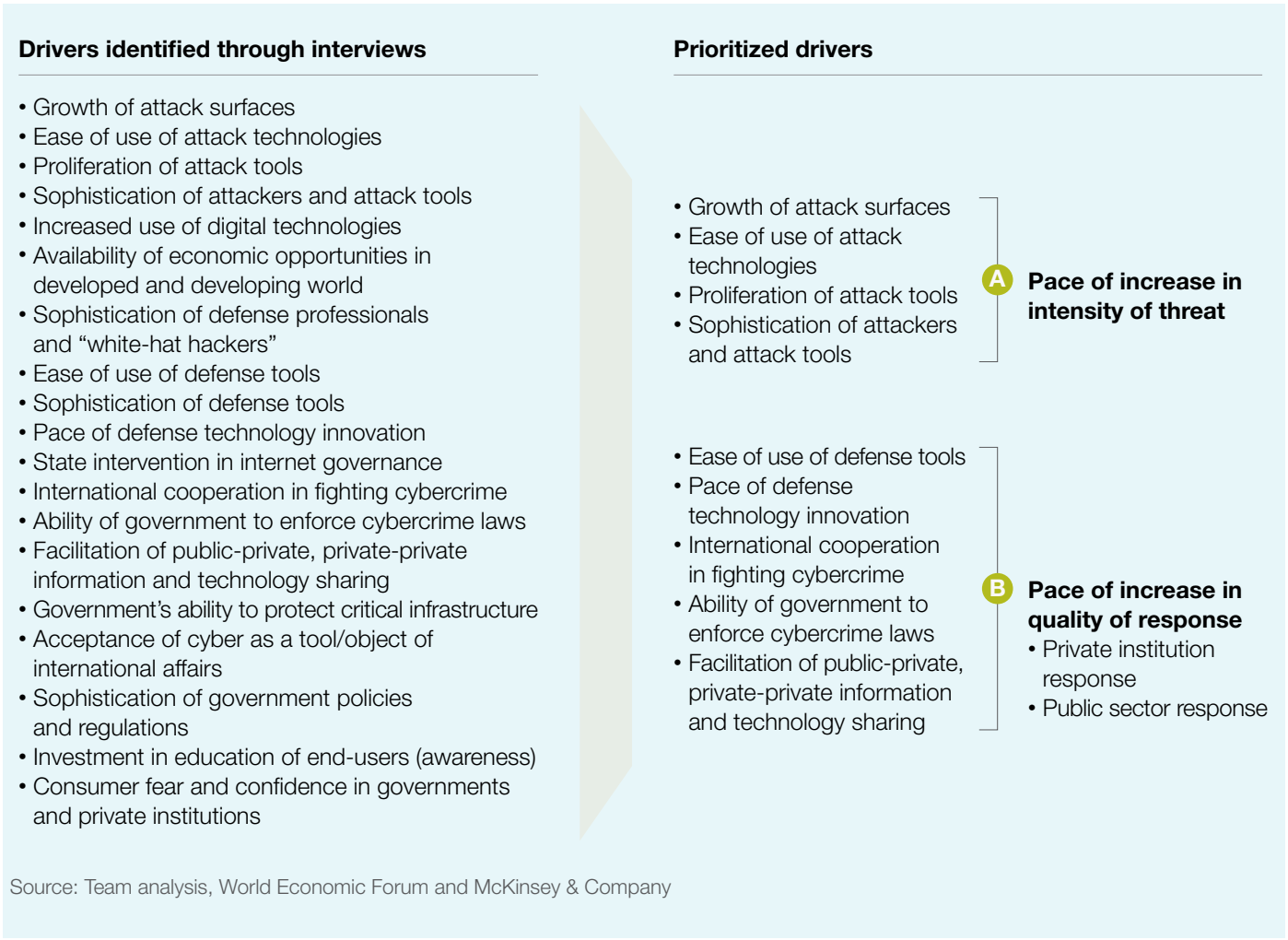
Christopher Mondini, Vice-President, Stakeholder Engagement, North America & Global Business Engagement, ICANN

Scott David, Executive Director, Law, Technology and Arts Group, University of Washington

Peter Schwartz, Senior Vice-President, Global Government Relations, Salesforce

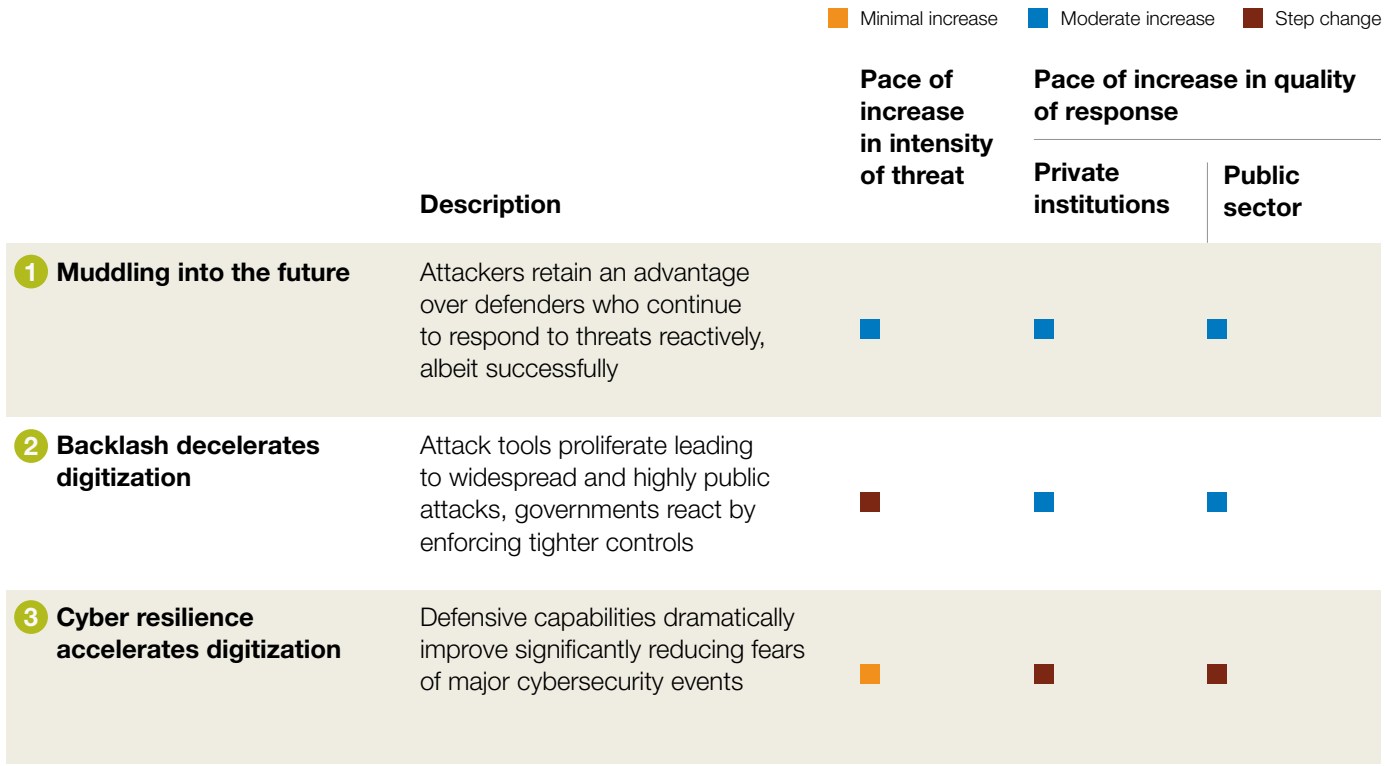
Christophe Nicolas, Senior Vice-President, Kudelski Group

FIGURE 11: TWO PRIMARY DRIVERS IN DEFINING FUTURE SCENARIOS



Source: Team analysis, World Economic Forum and McKinsey & Company

FIGURE 12: ALTERNATIVE FUTURE SCENARIOS FOR 2020



Chapter 3. Future Scenarios

The range of factors shaping the cyber resilience environment is vast, as the workshop sessions found. An analysis of possible outcomes must take into account a considerable degree of uncertainty. That said, scenario planning provides various potential ways in which the environment could develop.

On the future landscape of cyber resilience, the various dialogues identified dozens of shaping elements. These included such different drivers as the proliferation of attack tools, investment in educating end-users, international cooperation in fighting cybercrime, and the availability of economic opportunities in the developed and developing world. From this assortment, priority areas were distilled, and two essential drivers were defined of the future cyber resilience environment: pace of increase in the intensity of the cyber threat; and pace of increase in the quality of response from private institutions and the public sector. (See Figure 11.) A secure, robust cyber resilience environment spanning the public and private sectors would enable business and technology innovations, such as cloud computing and mobile Internet, to create between US$ 9.6 trillion and US$ 21.6 trillion in economic value between now and the end of this decade. But if that secure environment fails to materialize because rapidly increasing cyberattacks are met with less rapidly increasing defence capabilities, a backlash against digitization could leave as much as US$ 3.06 trillion of that value unrealized. Judging from the interviews and workshops, the executives believe that society is headed towards such a scenario, and that many components of that outcome are already beginning to materialize.

From this base and other extensive workshop sessions, three alternative future scenarios for 2020 have been created. The scenarios put cyber threats in sharper relief and form an economic value model that could be either achieved or threatened by an evolving cyber resilience ecosystem (see Figure 12). The three scenarios are:

- Scenario One: Muddling into the future
- Scenario Two: Backlash against digitization, prompted by proliferating cyberattacks
- Scenario Three: Accelerated digitization thanks to robust cyber resilience

Scenario One: Muddling into the Future

In this baseline scenario, attackers retain an advantage over defenders who continue to respond to threats reactively, albeit successfully. The level of threat rises incrementally, and a greater sophistication of attack tools consistently leaves defenders trailing. Institutions implement more stringent controls, but government intervention remains fragmented. No powerful international bodies emerge to coordinate the fight against cyber threats through the sharing of information and knowledge on attacker locations, intentions and strategies. Few cross-industry associations are effective in facilitating such exchanges.
At the operating level in this scenario, most business decisions likely are made without factoring in cyber resilience. Leaders continue to lack a clear grasp of the magnitude and nature of cyber threats. Senior business executives and company boards rarely engage with CISOs to consider the implications of business decisions on cyber resilience. Fragmented security solutions create operational inefficiencies such as slower transaction times. On the one hand, the potential advancement of new cyber defence technologies could hold out the opportunity for improved future security. On the other hand, fears of cyber resilience risks stemming from new business and technology innovations likely significantly delays adoption of those technologies, perhaps slowing global economic growth.

Scenario Two: Backlash Decelerates Digitization

In this second scenario, the frequency and severity of attacks is significantly increased, and international cooperation in combating the proliferation of attack tools and knowledge eludes efforts to bolster defences. More attacks aim to destabilize services (such as national payment networks) provided by private- and public-sector institutions. Government cyber resilience regulations become increasingly directive, forcing strict industry- and country-specific compliance to complex new mandates. Governments raise barriers to cross-border flows of information and technology. Defence takes the form of siloed initiatives and limited information-sharing. Consumers become increasingly cautious, curtailing use of mobile technologies for banking and other services.

Company operations under this scenario feel more exposed and restricted. As attacks escalate, cyber resilience teams increasingly deploy systems with inherent vulnerabilities, thus playing “catch-up” with attackers. Responses are hampered by a lack of institutional knowledge-sharing. Stringent security measures limit enterprise productivity and hinder innovation. Fears of cyber risks significantly delay the adoption of new business and technology innovations. Over time, the higher barriers to cross-border movement of information and technology hamper the efficiency of world trade and corporate resource allocation.

Scenario Three: Cyber Resilience Accelerates Digitization

In this third scenario, proactive public- and private-sector action limits the proliferation of attack tools, builds institutional capabilities, and stimulates innovation and economic efficiency. Formalized national cyber resilience legislation is paired with international collaboration to investigate and prosecute cyberattacks. International government coordination strengthens trust among individual institutions, allowing the establishment of stronger standards, greater cross-border collaboration and information exchange. International bodies emerge to coordinate the battle against cyber threats, leading to a more integrated global defence. Institutional capabilities grow, information exchange increases, and the adoption of innovative technologies accelerates.

This scenario offers a vital cyber resilience ecosystem that enables and connects company operations. Senior executives and company boards tap into expanding collaboration between public and private entities. Cyber resilience becomes more important on the C-suite agenda, and executives actively engage with CISOs on the implications of business decisions on cyber resilience, such as entry into new markets or outsourcing agreements. More sophisticated cyber resilience practices and technologies allow institutions to contain emerging threats. Enhanced defences against cyber breaches permit companies to connect more effectively with customers. Companies and consumers adopt innovations more quickly and freely. Information moves more easily across borders, enhancing the efficiency of trade and resource allocation.

Applying the Scenarios

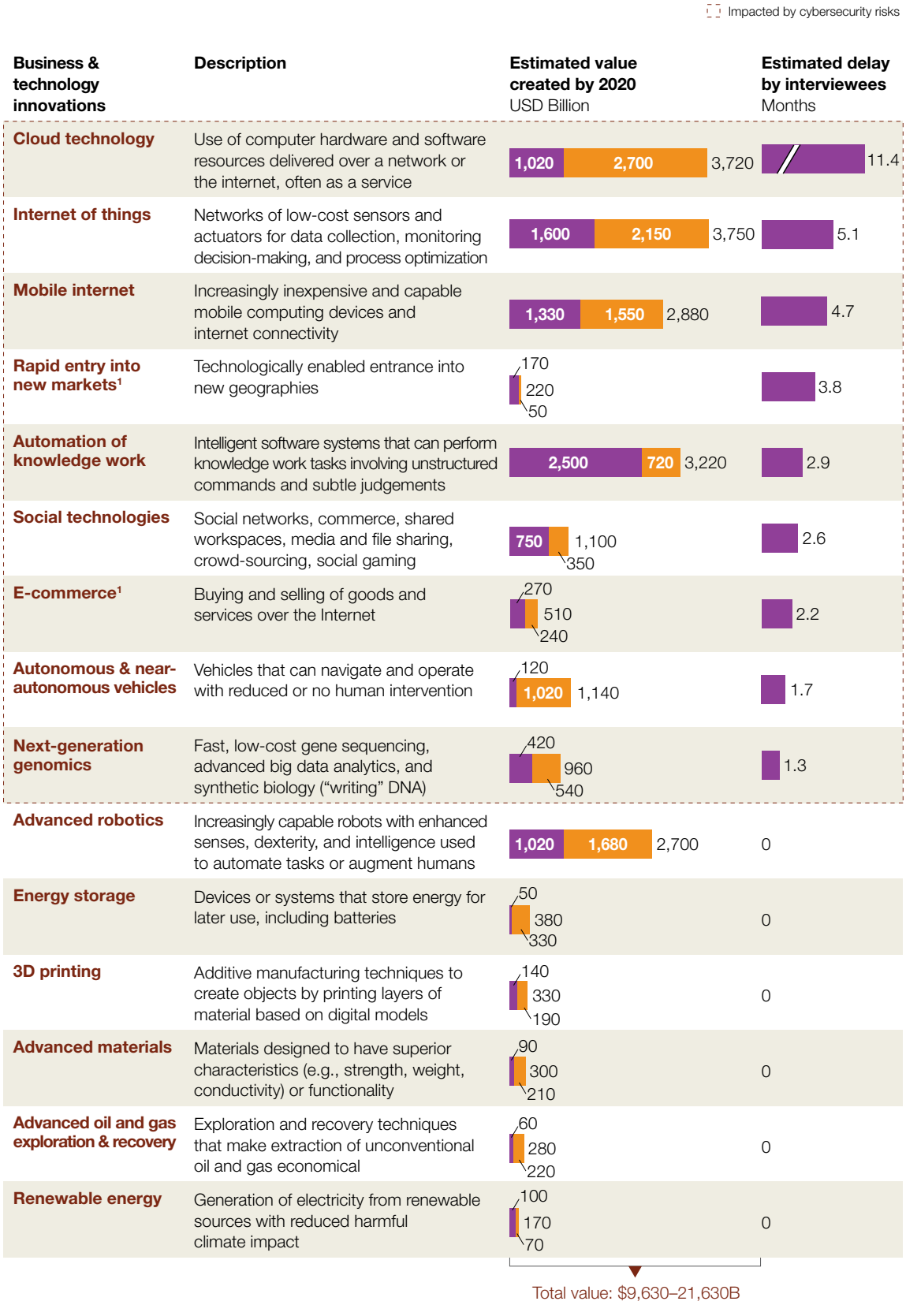
The output of the research and extensive partner workshops builds upon the work of the McKinsey Global Institute (see box) and other earlier efforts. It applies the three scenarios, estimating for each the economic value to be realized or lost as cyber resilience readiness affects adoption of business and technology innovations. Overall, it is estimated that these technologies represent between US$ 9.6 trillion and US$ 21.6 trillion in potential value creation by 2020. Yet even in the baseline scenario, in which the intensity and pace of cyberattacks increase only incrementally, the executives interviewed expect significant delays in implementing many of the most valuable business and technology innovations. (See Figure 13.)

In 2012 the McKinsey Global Institute set out to identify the technologies that over the next decade would truly matter to business leaders as they planned strategies, and to policy-makers as they tried to understand how technology would shape the global economy and society. The research focused on the speed, scope and economic value at stake from a dozen economically disruptive technologies — among them, cloud technology, the mobile Internet, and the networks of low-cost sensors and data collection and monitoring, commonly referred to as the “Internet of Things.”

MGI Disruptive Technologies report 2012

Calculated across the full range of some of these innovations, the risk of delays to adoption due to cyber threats could carry a high price tag for the global economy. In the scenario in which private and public institutions “muddle” into the future, the shortfall in estimated value created by 2020 could reach as high as US$ 1 trillion. And in the scenario where the private- and public-sector response to cyberattacks prompts a backlash against digitization, the impact on the global economy could amount to as much as US$ 3.06 trillion in unrealized value creation, or 14% of the total potential value creation of those technologies. (See Figure 14.)

FIGURE 13: POTENTIAL IMPACT OF CYBERSECURITY RISKS TO GLOBAL ECONOMY



[1]Estimated does not include consumer surplus

Source: MGI disruptive technologies, social economy & Internet Matters reports, UNCTAD direct investment, IMF global GDP, McKinsey Economic Analytics Platform, Industry leader interviews (100+)

FIGURE 14: FRAMEWORK FOR COLLABORATIVE ACTION

Impacted by cybersecurity risks

$ Billion	Est. value created by 2020	Impact of alternative future scenarios		
		Muddling	Backlash	Cyber resilience
Business & technology innovation total	9,630-21,630	(410)–(1,020)	(1,230)–(3,060)	Full value captured
Cloud technology	1,020 + 2,700[2]	(130)–(470)[4]	(390)–(1,410)[4]	-
Internet of things	1,600 + 2,150[2]	(90)–(210)	(270)–(630)	-
Mobile internet	1,330 + 1,550[2]	(70)–(150)	(210)–(450)	-
Rapid entry into new markets	170 / 50[1]	(10)	(20)–(40)	-
Automation of knowledge work	2,500 + 720[2]	(80)–(100)	(240)–(310)	-
Social technologies	750 + 350[3]	(20)–(30)	(70)–(100)	-
E-commerce	270 / 240[1]	(10)	(20)–(40)	-
Autonomous & near-autonomous vehicles	1,020[2] / 120	(20)	(10)–(70)	-
Next-generation genomics	420 + 540[2]	(10)	(20)–(40)	-
Advanced robotics	1,020 + 1,680[2]	-	-	-
Energy storage	50 / 330[2]	-	-	-
3D printing	140 / 190[2]	-	-	-
Advanced materials	90 / 210[2]	-	-	-
Advanced oil and gas exploration & recovery	60 / 220[2]	-	-	-
Renewable energy	100 / 70[2]	-	-	-

[1]Estimate does not include consumer surplus; based on IMF: April 2013 WEO data & MGI Internet Matters report; May 2011
[2]Based on MGI Disruptive Technologies projections for 2025 assuming linear ramp-up from mid-2013 to 2025 and scaling back to 2020
[3]Based on MGI Social Economy projections for mid-2012, extrapolated to 2020 based on 10-year average world GDP growth rate 2.6%
[4]>80% of impact for cloud is due to delayed adoption of public cloud

Source: MGI disruptive technologies, social economy & Internet Matters reports, UNCTAD direct investment, IMF global GDP, McKinsey Economic Analytics Platform, Industry leader interviews (100+)

Example. Consider cloud computing. In a best-case scenario, in which a solid cyber resilience ecosystem accelerates digitization, the private and public sectors see greater use of public cloud technologies, with enhanced security capabilities for non-critical workloads. Better use of private clouds handles critical workloads. Both public and private clouds continue to offer similar features. Enhanced security for private clouds comes at minimal performance penalty, and at a more noticeable performance penalty for public clouds. Under this case, cloud computing has the potential to create US$ 3.72 trillion in value by 2020.

In the baseline "muddling into the future" scenario, however, a different norm governs cloud computing's activity and economic potential. Use of public cloud technologies for non-critical workloads grows, as does use of private clouds for critical workloads. But fear of data breaches hampers use of public clouds for critical workloads. Delayed adoption of cloud computing means that between US$ 130 billion and US$ 470 billion of potential economic value remains unrealized.

Similarly, in the second scenario in which stepped-up cyberattacks, security gaps and a resulting rise in regulations create a backlash against digitization, public clouds are underutilized due to fears of vulnerabilities and higher costs from compliance with stricter policies on third- party access to data and systems. Achieving the full value potential of cloud computing is postponed by three years, and falls short by as much as US$ 1.4 trillion.

In coming years, annual spending on cyber resilience is likely to rise, from US$ 69 billion in 2013 to US$ 123 billion annually in 2020. But the extent of the increase and the return on investment will vary. In the best-case scenario, spending swells 13%, to US$ 139 billion annually, as public and private sectors lift defensive capabilities. In the worst-case scenario, in which US$ 3 trillion of potential economic value is unrealized, global spending nonetheless climbs 28% above the baseline scenario, to US$ 157 billion annually, as attacks step up and governments force compliance with increasingly complex regulations.

Chapter 4. Conclusions and Roadmap for Collaborative Action

The Forum's Partnership for Cyber Resilience, launched in 2012, recognizes the interdependence of public- and private-sector organizations in today's global, hyperconnected environment. Companies participating in this community-led initiative understand the importance of integrating cyber risk management into their day-to-day operations and of sharing information on threats and vulnerabilities.

As part of its multistakeholder dialogue across regions and sectors, the partnership also accepts that no static, universal set of actions can address the rapidly evolving environment of cyber risks. The community-led partnership has developed guidelines and principles for companies to build effective cyber risk management programmes. Included in the initiative is a framework tool for chief executive officers and other leaders to pilot internal reviews of their organizations' cyber resilience capabilities. The tool offers a rough composite score to locate the organization on the five stages of a "hyperconnection readiness curve". (See Figure 15.)

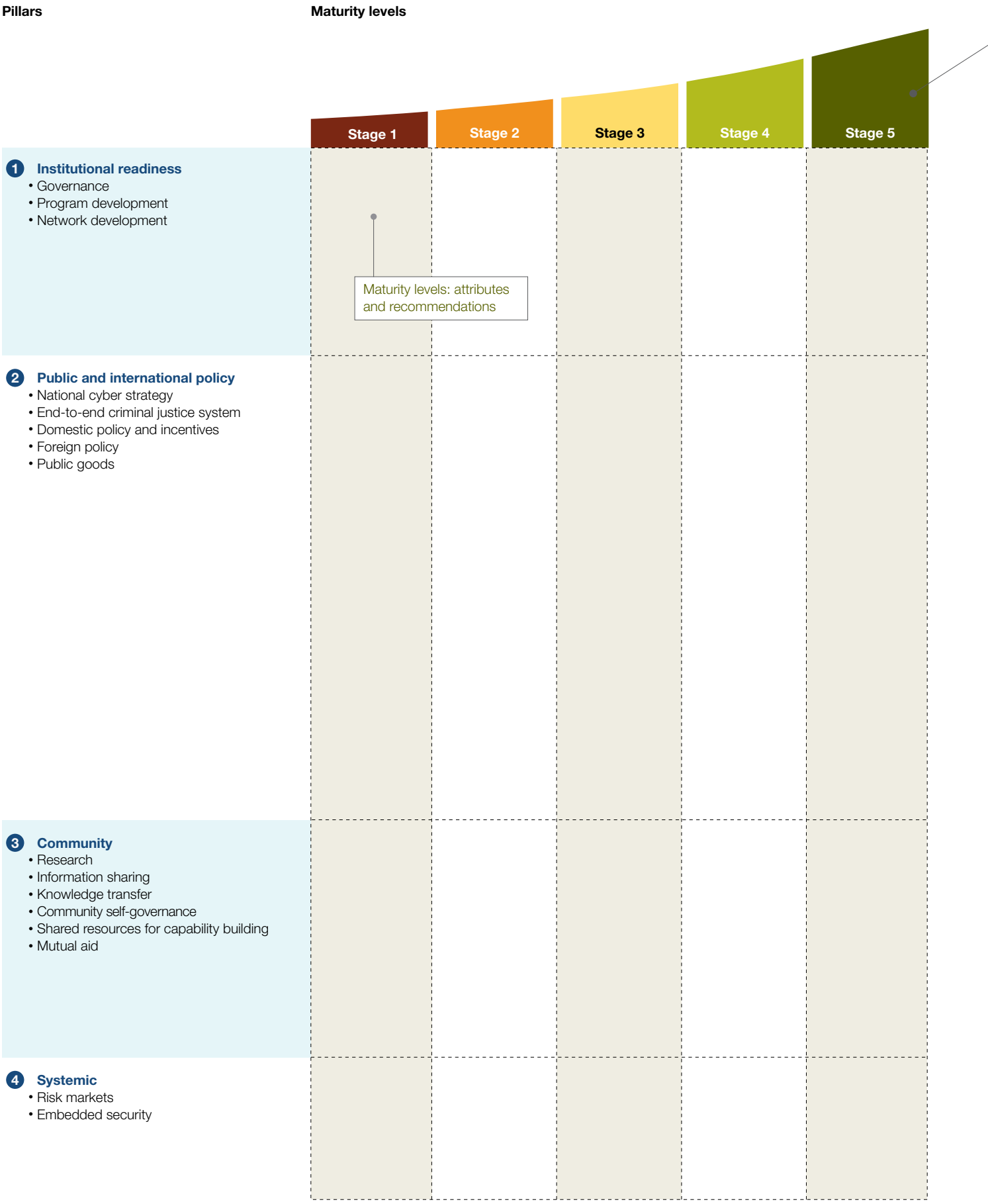
Against this curve leaders can aspire to select from a range of high-value responses to build a robust cyber resilience capability, and benchmark their institutions against best practice. The framework also can prompt discussion about the necessary steps to climb the maturity scale, the attributes against which to set goals, and the actions required to spur cooperation in building a stronger cyber resilience ecosystem. Finally, the framework can serve as a collaborative tool, providing a resource for member organizations through links to existing best practices and specialized organizations such as Interpol and Europol. The maturity-curve framework is a critical starting point for companies to position themselves on the scale of cyber resilience readiness, and the actions they can take to improve.

The next phase is to transform the static framework into a community-driven, self-sustaining online conversation. In this way, partners can facilitate the collection and synthesis of cyber resilience expertise across industries, sectors and regions.

With a core World Economic Forum team and its partners in an enabling role, the initiative engages participants by first locating their organizations on the cyber resilience readiness curve. The five stages of readiness range from "unaware" (companies that see cyber risk either as irrelevant or not part of their risk management processes) to "fully networked" (industry leaders in managing cyber risk). Organizations are advised on the precise steps necessary to move from one level to the next towards a vibrant networked approach to cyber risk management.
As strengths and weaknesses are identified, partners are encouraged to share their insights with one another and to actively adapt, improve and build out this framework so that it is broadly applicable and useful, regardless of sector or region. Simultaneously, the core team will proactively solicit input from partners who might have insights into specific sectoral cyber risk issues and remedies. The team will serve as a repository for those insights, which can then be used to flesh out the framework in a structured way for broader sharing. The idea is to create a continuous online feedback loop of ever-expanding knowledge to build the framework into a more precise barometer of an organization's cyber-readiness and to expand the range of constructive actions that public and private organizations can take to address gaps. Concurrently, a number of tools focus on specific components of the framework. The community is urged to link to these resources rather than create a new set of action items.

The Partnership for Cyber Resilience core team will organize regional meetings, project meetings and working group calls to launch and continue this community conversation, and provide the online tools for engagement to partners.

FIGURE 15: ROADMAP FOR COLLABORATIVE ACTION



Potential recommendations

Maturity curve from current Principles and Guidelines

Governance
- Prioritize information assets based on business risks
- Integrate cyber resilience into enterprise-wide risk management and governance processes and responsibilities
- Led in practice and policy from top leadership

Program/network development
- Provide differentiated protection based on importance of assets
- Develop deep integration of security into technology environment to drive scalability
- Deploy active defenses to uncover attacks proactively
- Continuous testing to improve incident response
- Enlist front-line personnel – helping them understand value of information assets

National cyber strategy
- Have a comprehensive and transparent national cyber strategy which Is integrated with the strategies and procedures all policy domains
- Strategies should incorporate private and civil sectors and should incorporate economic and security issues
- Establish a competent institution for the national strategy implementation and rollout

End-to-end criminal justice system
- Law enforcement has the capability and resources to investigate cyber crimes
- The state has an appropriate, comprehensive, and agile legal code for investigating and prosecuting cyber crimes
- Legal advocates understand the cybersecurity ecosystem well enough to carry out due process

Domestic policy and incentives
- Private, public, and civil dialogue to develop appropriate coherent mix of policy and market mechanisms
- Governmental mechanisms support law enforcement's efforts and is appropriately agile

Foreign policy
- Establish a national cyber doctrine
- Identify persons at the local, state and national level responsible for cybersecurity
- Establish formal and informal channels of communication between law enforcement entities
- Create interoperability amongst national level entities responsible for cybersecurity
- Work to harmonize national and international policies surrounding the prosecution of cybercrime
- Establish a multi-stakeholder approach towards governance on this issue

Public good
- Ensuring evolving and robust incident response capability
- Increase investments in cybersecurity technical education
- Fund a cybersecurity research agenda
- Provide "safe harbor" protection for limited sharing of information among and between companies and government

Research
- Increase education and awareness
- Encourage research on enterprise and macroeconomic impact of cybersecurity to prioritize and focus policies
- Create an atmosphere in which white-hat research is encouraged

Shared resource for capability building
- Foster partnerships between governments and universities and private sector for skills development

Information sharing
- Where legally feasible, institutions find mechanisms for legal information sharing makes sense
- Improve the quality of the ISACs/ CERTS/ CIERTs and other information sharing venues
- Promote an interoperable, extensible and automated system for sharing
- Provide common protocols to inform of information regarding cyber events

Risk markets
- Expand reach and breadth of cybersecurity insurance markets

Embedded security
- Explore ways to create a more secure internet, e.g: The new HTTP 2.0 standard has built in security via encrypted data transfer. Or by allowing ISPs to block computers that are participating in Botnets or are otherwise corrupted
- Develop a methodology for quantifying the impact of cyber

ICT Industry Team

Alan Marcus
Senior Director
ICT Industries
alan.marcus@weforum.org

Derek O'Halloran
Head of IT Industry
derek.ohalloran@weforum.org

Elena Kvochko
Manager, IT Industry
Partnership for Cyber Resilience
elena.kvochko@weforum.org

Roshan Vora
Project Manager
Risk and Responsibility in a
Hyperconnected World
roshan.vora@weforum.org

cyberresilience@weforum.org

Acknowledgements

We would like to sincerely thank our partners for their valuable insights, thought-leadership, contribution to this report and the overall support of the Partnership for Cyber Resilience initiative

Working Group

Claude Boudrias	Director, Government Relations	CA Technologies
Rob Wainwright	Director	Europol
Mustaque Ahamad	Professor, Computer Science	Georgia Institute of Technology
Jeff Moss	Vice-President and Chief Security Officer	ICANN
Christophe Nicolas	Senior Vice-President, Head of Kudlelski Security	Kudelski Group
Haden Land	Vice-President, Engineering	Lockheed Martin
Belisario Contreras	Program Manager, Cyber Security	Organization of American States
JP Rangaswami	Chief Scientist	Salesforce
Rod Beckstrom	Chief Security Advisor	Samsung Group
Lindsey Held	Vice-President, Global Government Relations	SAP
Murat Sonmez	Executive Vice-President, Global Field Operations	Tibco Software
Dmitriy Ustyuzhanin	Chief Information Security Officer	Vimpelcom
Julian Sevillano	Global Head, Enterprise Risk Management	Visa
Guha Ramasubramanian	Head, Business Development	Wipro
Anne-Marie Zielstra	Director, International Relations, Cyber Resilience	TNO

Additional Contributors

Stephen Cross	CEO	Aon GRIP Solutions
Simon Gibson	Head, Cyber Security	Bloomberg
Ray Stanton	Executive Vice-President	BT Global Services
Mark Hughes	CEO	BT Security
Kirstjen Nielsen	Member	Catastrophic Risk Global Agenda Council, World Economic Forum
Xiaodong Lee	CEO	China Internet Network Information Center
Adam Golodner	Director, Global Security and Tech Policy	Cisco
Voelker Hinrich	Managing Director	Deutsche Bank
Mark Clancy	Managing Director, Technology Risk Management	DTCC
Heli Tiirmaa-Klaar	Head of Cyber Policy Coordination	European External Action Service
Udo Helmbrecht	Executive Director	European Network Information Security Agency
Tom Robson	Europol Cyber Crime Center	Europol
Philip Verveer	Senior Counselor, Office of the Chairman	Federal Communications Commission
Greg Schaffer	Executive Vice-President	FIS
Matthew Fleming	Fellow	Georgetown University
Jonathan Zittrain	Professor, Internet Law	Harvard University

Art Gilliland	Senior Vice President and General Manager, Enterprise Security Products	HP
John Suffolk	Senior Vice-President, Head of Cyber Security	Huawei
Patrick Jones	Senior Director, Global Stakeholder Engagement	ICANN
Noboru Nakatani	Director	Interpol
Timur Tsoriev	Vice-President, Government and Strategic Relations	Kaspersky Lab
Kevin Mahaffey	CTO	Lookout Mobile Security
Cristin Goodwin	Senior Attorney	Microsoft
Jay Sullivan	Chief Operating Officer	Mozilla
Anil Süleyman	Head of Cyber Defence	North Atlantic Treaty Organization
Kevin Lee	Head of Asia	Palantir
Richard Horne	Partner	Pricewaterhouse Coopers
Michael Fertik	CEO and Founder	Reputation.com
Peter Schwartz	Senior Vice-President	Salesforce
David Kirkpatrick	CEO and Founder	Techonomy Media
Allan Friedman	Fellow, Governance Studies	The Brookings Institution
Robert Rose	Executive Vice-President	Thomson Reuters
Vincenzo Iozzo	Principal Security Engineer	Trail of Bits
Tim Crosland	Head of Cyber Prevention and Information Law	UK Cabinet Office
Eduardo Cabrera	Incident Response Integration	US Secret Service
Yuecel Karabulut	Cloud Infrastructure and Platform Product Security Leader	VMWare
Ken Hall	Head, Vice-President, Head of Cyber Consulting	Wipro

Project Advisors

James Kaplan	Lead Advisor, Partner	McKinsey & Company
Allen Weinberg	Senior Partner	McKinsey & Company
David Chinn	Senior Partner	McKinsey & Company

Over 500 executives, experts and policy makers participated in the workshops, industry leader surveys and partners activities throughout 2013. We are deeply indebted to all of those who have provided their input and expertise across many sectors and regions globally.

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

The World Economic Forum is an independent international organization committed to improving the state of the world by engaging business, political, academic and other leaders of society to shape global, regional and industry agendas.

Incorporated as a not-for-profit foundation in 1971 and headquartered in Geneva, Switzerland, the Forum is tied to no political, partisan or national interests.

World Economic Forum
91-93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org